Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Management and Marketing

Bachelor Thesis

Security Decision Models for Mobile Applications

Nitesh sharma

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Nitesh Sharma

Systems Engineering and Informatics
Informatics

Thesis title

Security Decision Models for Mobile Applications

Objectives of thesis

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

The first objective will be to make a detailed study on decision models that has been used for IT security purposes. Secondly, the author will try to find out if there are any decision models used for application security. Then, the researcher will analyze and compare decision models based on desirable security criteria and alternatives. Lastly, there will be suggested the most suitable decision model for application security.

Methodology

The initial phase will comprise a detailed literature study on the various decision making methods that have been used for IT security purposes. The second phase will take 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. Evaluation of decision models will be carried out with the help of MCDM. Based on the evaluated results, the suggestion of the suitable decision model for application security will be provided.

The proposed extent of the thesis

35-40 pages

Keywords

Mobile applications, security models, MCDM, criteria

Recommended information sources

Andreas U. Schmidt, Giovanni Russello, Iovannis Krontiris, Shiguro Lian. (2012),” Security and Privacy in Mobile Information and Communication Systems”, Springer Heidelberg Dordrecht London New York, ISBN 978-3-3642-33392-7

Mu, E. and Pereyra-Rojas, M. (2017),” Practical Decision Making: An Introduction to the Analytic Hierarchy Process (AHP) Using Super Decisions V2”, Springer Cham, ISBN 978-3-319-33860-6

Radha Poovendran, Walid Saad. (2014),” Decision and Game Theory for Security”, Springer international publishing Switzerland, ISBN 978-3-319-12600-5

Expected date of thesis defence

2022/23 SS – FEM

The Bachelor Thesis Supervisor

doc. Ing. Ludmila Dömeová, CSc.

Supervising department

Department of Systems Engineering

Electronic approval: 16. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Head of department

Electronic approval: 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 30. 11. 2023

Declaration

I declare that I have worked on my bachelor thesis titled " **Security Decision Models for Mobile Applications** " by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break any copyrights.

In Prague on _____

Acknowledgement

I would like to thank and express my gratitude to my supervisor, doc. Ing. Ludmila Dömeová, CSc., for her guidance, encouragement, support and sound counsel during y thesis. Her insights and feedback were invaluable in shaping my research and writing. Finally, I owe a debt of gratitude to my family and friends, who encouraged me, cheered. me up and celebrated my achievements along the way.

Abstract

Mobile application security is very paramount in modern days. As application developers continue to integrate features and interactivity for mobile users, there are potential exposure to more cyber security threats. This triggers the need for appropriate decision-making process for the identification of the right features and approach to undertake the enhancement of app security. This study starts by introducing the concept of application security. An introduction to the application security model is provided. The introduction also includes the provision of information on the security decision factors that determine the approach or model to be used in choosing the right application security development approach. The study revisits the single criteria model and compares this with the multi-criteria models. Discussion and comparison on the applicability of these models is addressed from the reflective and research point. The study evaluates the compromise variant (CV) in the decision models and applies the SAW approach in MCDM models to dealing with the application security. Case studies and prior research are used to assess the use of the models for different conditions. A subsequent assessment of the reflections of the app developers and users will help in identifying the effectiveness of application security management models. A recommendation to the use of applicability of the AHP and TOPSIS decision model as a consideration under the compromise variant (CV) in the development of advanced security features has been discussed. The study draws a conclusion and recommends for further studies to deal with security features.

Keywords: Mobile applications, security models, MCDM, criteria

Rozhodovací Modely Zabezpečení Pro Mobilní Aplikace

Abstrakt

Bezpečnost mobilních aplikací je v dnešní době velmi důležitá. Jako vývojáři aplikací pokračují v integraci funkcí a interaktivity pro uživatele mobilních zařízení, jsou potenciálně vystaveni většímu počtu kybernetických bezpečnostních hrozeb. To vyvolává potřebu vhodného rozhodovacího procesu pro identifikaci správných funkcí a přístupu ke zvýšení bezpečnosti aplikací. Tato studie začíná představením konceptu bezpečnosti aplikací. Je uveden úvod do modelu zabezpečení aplikací. Součástí úvodu je také poskytnutí informací o bezpečnostních rozhodovacích faktorech, které určují přístup nebo model, jenž má být použit při výběru správného přístupu k vývoji zabezpečení aplikace. Studie se vrací k modelu s jedním kritériem a porovnává jej s modely s více kritérii. Diskuse a srovnání použitelnosti těchto modelů je řešena z hlediska úvah a výzkumu. Studie hodnotí kompromisní variantu (CV) v rozhodovacích modelech a aplikuje přístup SAW v modelech MCDM na řešení bezpečnosti aplikace. K posouzení použití modelů pro různé podmínky jsou použity případové studie a předchozí výzkum. Následné vyhodnocení úvah vývojářů a uživatelů aplikací pomůže při zjišťování účinnosti modelů řízení bezpečnosti aplikací. Bylo diskutováno doporučení k využití použitelnosti rozhodovacího modelu AHP a TOPSIS jako úvahy v rámci kompromisní varianty (CV) při vývoji pokročilých bezpečnostních prvků. Studie vyvozuje závěry a doporučení pro další studie zabývající se bezpečnostními prvky.

Klíčová slova: Mobilní aplikace, bezpečnostní modely, MCDM, kritéria

Table

1 Contents

of content

List of pictures

List of tables

List of abbreviations

AHP – Analytic Hierarchy Process

API - Application Programming Interface

COPRAS – Complex Proportional Assessment

CV – Compromise Variant

ELECTRE- Elimination and choice expressing reality.

MCDA – Multi Criteria Decision Analysis

MCDM – Multiple Criteria Decision-Making

NIS- Negative Ideal Solution

PIS – Positive Ideal Solution

PROMETHEE - Preference Ranking Organization Method for Enrichment Evaluations

TOPSIS – Technique for Order of Preference by Similarity to Ideal Solution

VIKOR – 'VlseKriterijumska Optimizacija I Kompromisno Resenje,' meaning multi-criteria optimization and compromise solution.

WSM – Weighted Sum Model

2 Introduction

A mobile application's performance may suffer because of selecting the wrong security type, resulting in vulnerable issues. Every issue may be a result of user or the manufacturing problem. However, the role of the installed programs and software plays a significant role and is a key decision point for mobile phone security (Jahkola *et al.*, 2017). Users have been empowered and influenced by the mobile revolution to move nearly all their day-to-day activities into the mobile environment and so-called mobile applications. Each mobile app perspective can be addressed when the evaluation is conducted from a viable approach to derive the best security option for mobile telephones especially for the applications (Gardner *et al.,* 2022). Decision making can be used to select the most viable security type to embrace and install or upgrade for applications.

The world of apps is changing with third-party and open-source libraries helping to speed up development and deployment. In this study, a focus on the MCDM approaches that can be applied by app developers in enhancing the security features is evaluated. An evaluation of the various MCDM models with a focus on the application of the models' considerations is utilised. Ultimately, each decision mechanism is assessed based on the ability to deal with security features deployment in the making of the apps (Strzelecki, 2020). Besides, the considerations made in the attainment of the decision for the integrated mechanisms is discussed with the use of comparative variance is used in selecting the most appropriate mechanism for the app security considerations by the developers. The findings of this study show that more advanced approaches, such as the technique for the order of preference by similarity of AHP and WSM in comparison to TOPSIS and PROMETHEE, are better able to predict which apps will be used to determine app security. A conclusion is drawn from the information shared in the report.

3 Objectives and Methodology

3.1 Main Objectives

The main for this study is to evaluate the decision models that can be used in the development of a reliable IT security features by the mobile application developers.

3.2 Other objectives

- Find out the existing IT security decision models applied by Mobile Application developers.
- Analyse and compare available decision models used in mobile application development.
- Evaluate the compromise variant (CV) for the MCDM models.
- Recommend strategies of deploying better IT security solutions for the Mobile application developers

3.3 Methodology

The initial phase will comprise a detailed literature study on the various decision-making methods that have been used for IT security purposes. The second phase will take 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. Evaluation of decision models will be carried out with the help of MCDM. Based on the evaluated results, the suggestion of the suitable decision model for application security will be provided. This study is a secondary exploratory study evaluating the consideration by the mobile app developers in terms of the most appropriate decision-making approach to use. The interpretivism philosophy is applied with a deductive approach being adopted. The multimethod qualitative method choice is used focusing on archival research within a cross-sectional time horizon. Data garnered from the secondary studies and in relation to the application of decision-making approaches is analyzed using the WSM and

AHP methods and a compromise variant developed at the results and discussion levels of the report.

4 Literature Review

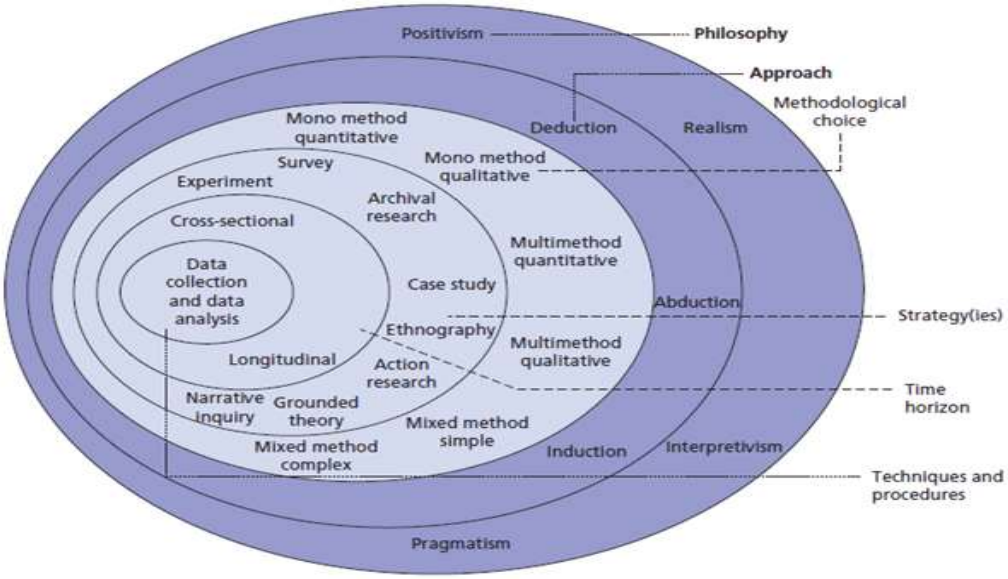
4.1 Statement of Problem

Information security managers must not only clarify pertinent information but also consider its interdependencies. When dealing with a dynamic field such as the development of mobile applications, the management and team must be ready to ensure that there is sufficient information to help in deciding the way forward for any organization. The collection of ideas and the roles of the decision models cannot be overlooked in such a sensitive field. Moreover, the connection between the application developers' efforts and the desire to implement adequate security measures has not seen the attackers unable to breach the application's security (Gardner et al., 2022). They still gain access to mobile applications due to the inadequate selection of application security types. Most modern mobile operating systems, including iOS, Android, and Windows Phone, make it simple to install modern mobile applications. There is a general observation of an increase in the number of complex-problem-resolving, advanced, and individualized applications on the market because of fierce competition among application providers. According to Karande and Joshi (2022) the software development market has seen a rapid expansion of mobile developer and user domains, which are essentially key in the ultimate realisation of secure or more resilient applications. MCDM looks at the criteria to figure out if each one of available options is a good or bad choice for a particular application.

4.1.1 Study Design

This study is a secondary exploratory study evaluating the consideration by the mobile app developers in terms of the most appropriate security criteria to use. The multi-method qualitative method choice is used focusing on the archival research within a cross-sectional time horizon. Data garnered from the secondary studies and in relation to the application of decision-making approaches is analysed using the WSM and AHP methods and a compromise variant developed at the results and discussion levels of the report.

Figure 1:Research Onion by Saunders (2012)



Source: Saunders (2012)

The qualitative methods chosen for this study is the WSM and AHP as MCDM methods of decision making. They will be applied in regarding the valuation model based on the factors raised by mobile application developers. The analysis thereby is provided as a guide to ultimately developing the comparative variance of the decision models. Figure, tables, and Charts are provided to summarise information into infographics.

4.1.2 Data collection and Analysis Methods

The study is carried out using mixed methods with the initial phase to extract information from secondary studies in order bring about the basis of conducting this study. The literature review forms the basis of evaluating the MCDM methods and how they relate to the derivation of reliable decisions by engineers and other professionals. Charts, graphs, and summaries of explanatory information regarding MCDM is provided. The Information from this was used to develop the question that was used in evaluating the opinions of the app developers which is then presented in discussions, tables, charts, and figures. According to Borissova (2021), open-source code can make up the highest percentage of enterprise apps. Unfortunately, vulnerabilities that enable attackers to remotely exploit a system have frequently been caused by third-party code. It is possible to decompile open-source software.

To assess the significance of such, the use of tools helps in engaging the respondents in handling the desired quality of security features within the apps.

App developers can build an app from the ground up and make it harder for people to reverse engineer it is using new, secure codes. For employees who log in to applications remotely, businesses can use virtual private networks (VPNs) to add a layer of security to mobile applications (Costa *et al.*, 2019). The development of security measures for the applications can be evaluated in a manner that focuses on how the decisions are derived. These presentations are meant to help in summarising the existing data and the gaps that exist in the MCDM models. Data collected is shared as summaries, charts, and graphs. This information is then interpreted into useful information that is used to derive the ultimate consideration made on the appropriateness of the MCDM methods, in making decision to manage the security matters by app developers.

4.2 Mobile app security Framework

The world of mobile devices has seen tremendous change in the last few years, which has resulted in a significant rise in internet accessibility while using mobile devices instead of traditional desktop systems. According to the growing importance of smartphone the use of mobile applications is also Increasing rapidly. Mobile applications are an essential part of our everyday lives in the connected world. These applications bring a level of accessibility and ease in our daily life from social networking, travelling, banking to healthcare management. The necessity of mobile app security has increased rapidly along with the increasing number of mobile applications. App developers and users now have serious worries about protecting sensitive data, maintaining user privacy, and battling cyberattacks. This means that dynamic threat identification and defense has become essential to the security of mobile applications. Rather than depending on a more conventional implementation in the structures on the device, or in the network, these measures need to evaluate risks dynamically at the point of access. To put it further, trust needs to be built dynamically in the present mobile period rather than dynamically decided.

4.3 Factors of Decision Making for Mobile Applications Developers

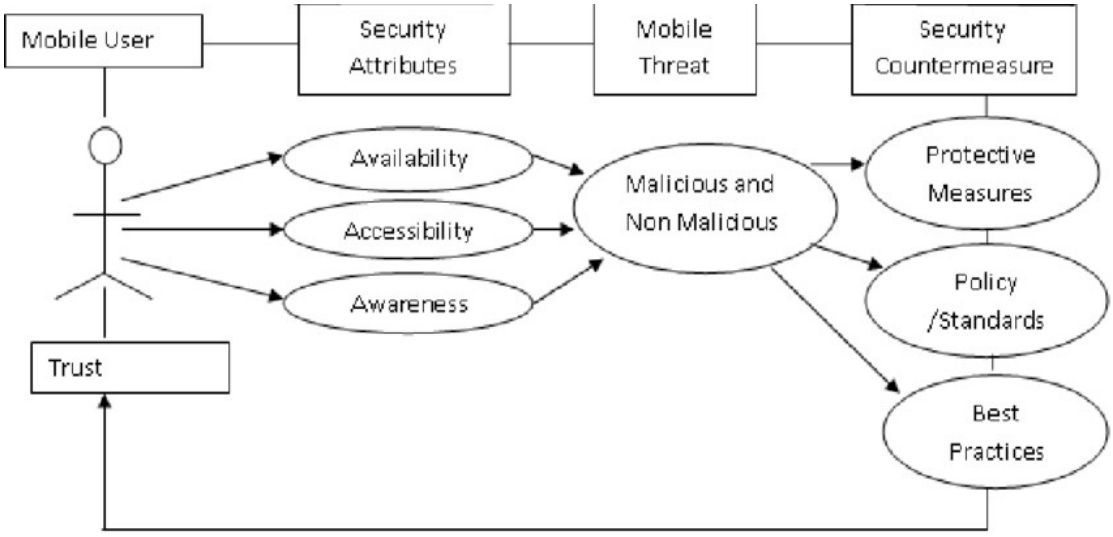
Making decisions is a difficult task for humans. It is difficult to determine which one or a set of alternatives with multiple criteria is the best when choosing one. When selecting a security type for a mobile application, developers must incorporate Multi-Criteria Decision Making (MCDM) Models (Kabassi, 2022). The application of MCDM models is mainly concerned with the provision of decisions supported by a criterion viable strategy to uncover the threats and embrace new ideas. For mobile app developers, a decision model for application security makes it easier to choose and set the necessary application security types (Han *et al.*, 2016). In selecting the best security measures for mobile applications, we have considered seven criterions which are most important to a user to decide which security measure is best from the provided set of alternatives. The criteria are Security Impact(C1), Exploitation Time(C2), Implementation Time(C3), Maintenance Time(C4), Effectiveness(C5), Adaptability(C6), and Adverse Effect(C7).

4.4 Decision Making Models

There are two types of decision-making models: single-criteria and multi-criteria approaches. To ensure that mobile applications meet the operating system's security requirements, developers must take these security decision models into account. Users of mobile devices view them as very personal tools that are mostly used to make everyday tasks easier, but they also store very private personal information. It's essential to be aware of apps' security issues (Strzelecki, 2020). Reviews are an important way for users to learn about various app issues. A limited number of existing reviews have been used in previous studies to provide a comprehensive summary of the app's security issues. Review classification has been automated using machine learning (ML) algorithms according to classes (Strzelecki, 2020). These intelligent algorithms need a lot of data, which takes a lot of time and effort. The results are greatly influenced by the quality of the manual annotation. To some extent, research studies and business organizations have developed and promoted best practices to address this growing problem (Sarker *et al.*, 2022). As a result, the purpose of this study is to compare current best practices with security threats to mobile applications.

One main alternative is that of making decisions that compensate weaknesses with enhancing the strengths of a given option. This alternative involves evaluating the criteria, considering both their strengths and weaknesses, and allowing the strengths of each criterion to make up for the weaknesses, thereby considering all of the criteria. The analytical hierarchy process (AHP) is an example of a compensatory decision-making tool (Khan et al., 2021). This method is mostly used when the environment for the analysis is complex. The method can be applicable when evaluating issues whose main decision may touch on bearing less impactful weaknesses in a project (Karande & Joshi, 2022). It is used when comparing difficult-to-quantify criteria. The ultimate decision to enhance the stronger aspects is realised within a shorter period as opposed to long-term decision processes. The basic is to reflect on the threat model (see figure 2 below) that can make the application of the appropriate decision model for the application developers.

Figure 2: Threat Model in Application Development



Source: Gardner *et al.* (2022)

Making long term security decisions can be done using other MCDM options. Another alternative is that of prioritising the process of making decisions. To determine which criteria, rank higher than the others based on the comparisons, focuses on the approach to prioritising decisions and this offers a method that compares the criteria for the pairs of information. One of such methods is the elimination and choice expressing reality (ELECTRE) (Khan et al., 2021). This is a technique for selecting, ranking, and sorting

options to solve a problem, is a well-known example of an outranking decision-making method.

Advances in hardware, software, networking, processing, and communications have completely changed the field of information technology (W Saad,2014). Key security indicators have a direct effect on an organization's security status, while other indicators only have an indirect connection. To take the right and effective measures to reduce threats, managers need to be able to consider not only technical threats but also other factors like human behaviour. Information security managers should be aware of both direct and indirect MSFs to make appropriate decisions based on these findings (Tan et al., 2021). The Security-Related Review (SRR) Miner, AR-Miner, or SUR Miner models can be used to assess user feedback (Suomalainen, *et al.*, 2022). SRR-Miner begins by extracting security-related reviews using a keyword-based method. It then extracts from review sentences, based on predefined semantic patterns, words that represent misbehaviours, aspects, and opinions.

4.5 MCDM in Security Level Modelling for Mobile Applications

Application security refers to security measures implemented at the application level with the intention of preventing the theft or hijacking of the app's data or code. Hardware, software, and procedures that identify or reduce security flaws may all be part of application security (Strzelecki, 2020). The security includes both the systems and methods used to safeguard apps after they are deployed and the security concerns that arise during application development and design. Hardware application security refers to a router that restricts Internet access to a computer's IP address (Daradkeh & Sabbahein, 2019). However, security measures at the application level are frequently incorporated into the software as well, such as an application firewall that precisely specifies the kinds of activities that are permitted and those that are not (Jahkola *et al.*, 2017). An application security routine that includes protocols like regular testing is one example of a procedure. When determining the kind of security features that are incorporated into the application, each of these aspects plays a crucial role.

Information security management is frequently developed in accordance with international standards or best practices. From the perspective of management, vulnerabilities are typically of a technical nature. This is because they are known system vulnerabilities and software is designed to deal with them (Costa *et al.*, 2019). Experts agree that vulnerability is a problem caused by unpatched systems and a subject for patch management. Vulnerability scanners, penetration tests, automatic scans, audits, and the definition of toxic software found on systems are used to evaluate them. Based on the evaluation methods provided, vulnerabilities are patched and eliminated.

Management's knowledge of an application's assets and infrastructure, including its vulnerabilities, presents a challenge in practice. It is possible to determine whether vulnerabilities are known if an application has complete access control of its assets and infrastructure (Daradkeh & Sabbahein, 2019). When security and performance are considered, resource allocation is an important factor. Depending on the security type, the application developer must consider the number of resources used, such as operating memory and connectivity speed. Security planning must be aligned with the larger objectives of the application and so managerial support for security is crucial.

In addition to ensuring that adequate features are integrated and that the organization's broader plans are adequately considered, application security management must ensure that the security policy adheres to the existing rules, regulations, and laws. Most of the time, traditional computer security approaches focused a lot on preventing attacks on systems and reducing the likelihood of software and hardware failures (Gardner *et al.*, 2022). According to Daradkeh and Sabbahein (2019), the developers simulate the use cases that can cause incidents and they use these to gather evidence of incidents occurring, safeguard the user's valuable information, or prepare for system recovery or enhancement of the security features. A little thought was usually given to how to deal with an attack or failure once it occurs. As a result, many decisions were made hastily when a problem arose. This lack of forethought is often reflected in modern decision approaches.

Users can log in to all online resources, websites, and apps by using authentication. However, not all authentication methods are created equal. The most common usernames and passwords are also among the most vulnerable to hackers. They are able to gain access to user accounts by using brute force, credential stuffing, and bots, as well as long, secure passwords (Jahkola *et al.*, 2017). The bottom line is that passwords won't work in the future.

Integrating biometrics like fingerprint and face IDs into apps and websites is a better option for multi-factor authentication. Additionally, they use SSL to safeguard access credentials and session identifiers and help to protect session data (Han *et al.*, 2016). It may be easier to prevent attackers from completely gaining access to the system if you take the time to secure the authentication procedure.

Picking an unseemly security type for a portable application might prompt execution debasement and weak issues in applications. The decision of the security type should be possible by direction of adopting technology that makes unwarranted navigation a difficult errand for fraudsters (Costa *et al.*, 2019). While picking a solitary option among a bunch of choices with various standards, it is difficult to tell which one is the better choice. Portable application engineers need to consolidate Multi-Standards Independent direction (MCDM) Models to pick a reasonable security type for versatile application (Karande & Joshi, 2022). A choice model for application security upgrades decision making for versatile application engineers to choose and set the necessary security types for the application (Gardner *et al.*, 2022). A comparative of the relevance of each of the MCDM models can be seen in Figure 3 below. In the field of data innovation, choice models have been applied for Data Security, network security, application security reason.

Table 1: Comparison on the Attributes of some MCDM Methods

Method	Description	Crisp/fuzzy	Average/voting
WSM	The weighted sum is estimated using the averaged weight from individual DMs and the averaged performance value	Crisp	Average
TOPSIS	The relative preference defined by TOPSIS is estimated using the averaged weight from individual DMs and the averaged performance value	Crisp	Average
Fuzzy TOPSIS	The relative preference is estimated using the fuzzified weights from individual DMs and the fuzzified performance value	Fuzzy	Average
Group TOPSIS	The relative preference is estimated with internally integrating weights from individual DMs	Crisp	Average
TOPSIS-Borda	Borda counts are estimated after applying TOPSIS for individual DMs (multiple TOPSIS with the weights from individual DM)	Crisp	Voting
TOPSIS-Copeland	Copeland's counts are estimated after applying TOPSIS for individual DMs	Crisp	Voting

Source: Tan et al., (2018)

However, there has been no work done on the compromise variance for the decision models applied in deciding on application security. As an innovative digital technology, building Information Modelling (BIM) was an approach used previously and was anticipated to revolutionize the conventional information management procedures by focusing on a compromising regard to the decision process (Tan et al., 2018). Specifically, the incentive of BIM makes it possible to integrate the fragmented architecture, engineering, and construction (AEC) industry by vertically integrating information at various stages and horizontally integrating stakeholders (Tan et al, 2018). The integration meant creating a balance in the manner the decision would balance in ensuring the safety of such projects. BIM models contain both geometric and non-geometric data. BIM can quickly and precisely extract information from components and assist in evaluation by integrating data from various fields by accepting some and eliminating some.

In the design and development of any product, choosing the appropriate creation method is a difficult issue. According to Gardner *et al.* (2022), the decisions to enhance the products from the existing to a new level demands a collective check on the attributes for

each of the determining factors among other determinants. In addition, a wider scope view it is essential for successful outcomes, cost reduction, and improved performance (Ettiane et al., 2021). The AHP, TOPSIS, and VIKOR are just a few of the various approaches that have been suggested in literature as potential decision-making models that regard the various weights in decisions versus the value of every option (Bhole, 2018). However, a few studies have conducted comparative studies of these approaches in relation to the issues of selecting development processes (Daradkeh & Sabbahein, 2019). Some have been done on manufacturing process and others have just been focused on hardware elements. Thus, the desire to have more application of the decision models in the modern society is to help in the enhancement of the decision process for the software components of organisations.

Significance of each model range from the application development to the development of resilient application features for computational complexity, decision-making agility, the number of alternative processes and criteria. These also reflect on the adequacy in supporting a group decision on addition or removal of a criterion used to evaluate the MCDM approaches (Bhole, 2018). Typically, the application of this methodology is evaluated in a real case study. Productivity, accuracy, complexity, adaptability, material utilization, quality, and operation cost are identified as the criteria used to evaluate the most suitable manufacturing process or a process that involves technical developments (Strzelecki, 2020). In the long run, these factors may lead to the adoption of a contributory decision that is more engaging.

The choice of a single technique or mix of strategies is a difficult task which relies upon kind of choice issue. The various MCDA techniques assist with distinguishing when a more favourable condition whereby a specific strategy is reasonable (Bączkiewicz et al., 2021). The mobile technology developers introduced the most common way of demonstrating and organizing assumes a significant part of any choice guide philosophy. In BIM-based decision-making processes, Multi-Criteria Decision Making (MCDM) has begun to demonstrate its capacity to integrate technical information and multi-stakeholder value (Khan et al., 2021). By combining component and frequently conflicting indicators from all information sources into a single overall indicator, it compares and ranks decision-making schemes.

The application on MCDM models in decision making has been identified as depending on the kind of model that they are being applied. Some of the models may be

significant in the development of structures that are within a given sector (Karande & Joshi, 2022). Others may be relevant to several sectors and can be combined for evaluation of decisions within same section. The figure 4 below indicates a comparative analysis of the application and combination of models in a study conducted by Bhole (2018). In the study, Bhole evaluated the merits and application of various models and uncovered the significance of each model on the various sectors within which they same were applied (See Figure 5 Below). The study laid a foundation for future engagement in connecting the models with each sector in which they are termed relevant. Besides, Bhole (2018) gives an account of challenges within the select models. These are areas where further studies can be developed to assess potential means of overriding the demerits in the decision models.

Table 2: Sectors for Applying the MCDM Models in Decision Process

MCDM Method	Merits	Demerits	Applications
Multi-attribute utility analysis (MAUT) Churchman, C.W., Ackoff, R.L. and Arnoff, E.L. (1957)	• Takes uncertainty into account; • Can represent the uncertainty directly to decision model • It has a strong form of decision making Simple to method • Easy calculations. • The mechanism of the method is straight forward	Needs a lot of input; preferences need to be precise.	• Public Sector like, new airport, forest land use • Power Plant related selection. • Supplier selection • Economics, finance, actuarial, water • Management • energy management • agriculture • E commerce • Truck load condition. • Motion simulator. Global manufacturing (canbolt Chelst Garg 2007) Social problem Land use Natural resource management Technical socio-cultural for eight countries(Ananda and hearth 2005) Watering system(kailiponi 2010) Soil contamination (zabeo)
Analytic Hierarchy Process (AHP) Saaty, T. L. (1977).	• Easy to use; • handle the multiple measures and perspectives • scalable; • hierarchy • structure can easily adjust to fit • many sized problems; not data intensive.	Problems due to interdependence between criteria and alternatives; can lead to inconsistencies between judgment and ranking criteria; rank reversal.	• Supply chain Management. • Transportation • Resource management • Health Technology • corporate policy and strategy. • public policy, • Industrial robots • Selection of Techno-Entrepreneurship Projects • political strategy, and planning. • Fisheries • Infrastructure. • Water resource management
Case-Based Reasoning (CBR)	• Not data intensive; • can adapt to changes in environment.	Sensitive to inconsistent data; requires many cases.	• Health • Insurance • Identifying knowledge leader.

Source: Bhole (2018)

A set of security strategies that prioritize mobile devices has emerged as a result of this approach's widespread adoption. Writing reliable code, which will assist you in protecting your app from attackers, is the simplest way for app developers to ensure the security of mobile applications (Wu, 2022). When using third-party libraries in an app, it is recommended that you test the code before using it to ensure the highest level of security. Application developers desire to have effectual policies that can determine how to handle libraries and limiting the number of libraries used in a code through embracing systems or

approaches to sound decisions (Teymourzadeh et al., 2017). Therefore, following the rising cases of security challenges facing the app developers, the need for appropriate coding can be determined through application of desirable MCDM models.

Applications that use firewalls that are porous run the constant risk of being hacked. There are a record number of data leaks in the last decade, though the numbers have gone down with constant upgrades (Maliene et al., 2018). However, data leaks are still a big problem for application developers especially in the mobile phone category. Additionally, server-level security and user data storage may be in jeopardy if API integration is not properly monitored. Scams are quite common because any application designed to handle financial transactions is always susceptible to fraud (Song *et al.*, 2018). As a result, every application must operate within a social and legal framework. Users may fall prey to the ever-increasing threat of cybercrime if security mechanisms and decisions are not appropriately adopted. Due to the ever-increasing popularity of mobile phones, mobile-first design and development has emerged as the most common method.

As part of the software development process, application developers conduct application security testing to ensure that new or updated software applications do not contain security flaws. According to Maliene et al. (2018), security audit can verify that the application satisfies a particular set of security requirements. Developers need to make sure that only authorized users can access the application after it passes the audit. In penetration testing, a developer looks for ways to break into the application by acting like a cybercriminal (Teymourzadeh et al., 2017). Social engineering or attempting to deceive users into allowing unauthorized access is examples of penetration testing methods. Unauthenticated and authenticated security scans are frequently carried out by testers.

Application developers can make it easier to ensure mobile app security is heightened by establishing a policy prohibiting the use of such third-party components. To have secure code, regular testing and bug fixing of mobile app security is also essential (Sarker *et al.*, 2022). Best practices for mobile app safety are constantly evolving and becoming more sophisticated as technology advances. As a result, methods for ensuring the security of mobile apps have evolved over time. The best way to ensure the safety of mobile applications is to learn how to protect your phone and be aware of the risks posed by security issues (Samantraj et al., 2020). Security can be greatly improved through secure coding practices, continuous security testing, penetration tests, and a focus on satisfying user experiences. The

app's cache manager should clear data whenever it is running in the background, even though password access to the app significantly reduces the likelihood of this occurring. Therefore, every time the device reboots or another user logs in, the cache data ought to be automatically deleted.

Perhaps a key issue that IT administrators and application developers must address on the long term is the resilience in networks or application security. Cyber security reports indicate that there are some attack vectors that cybercriminals typically use to penetrate corporate networks or even applications (Maliene et al., 2018). Strzelecki (2020) notes that a high number of such leads to uncompromising need to proactively deal with security issues and threats as they arise daily. It becomes necessary to identify elements and components within the network security access control and authentication method to address such issues.

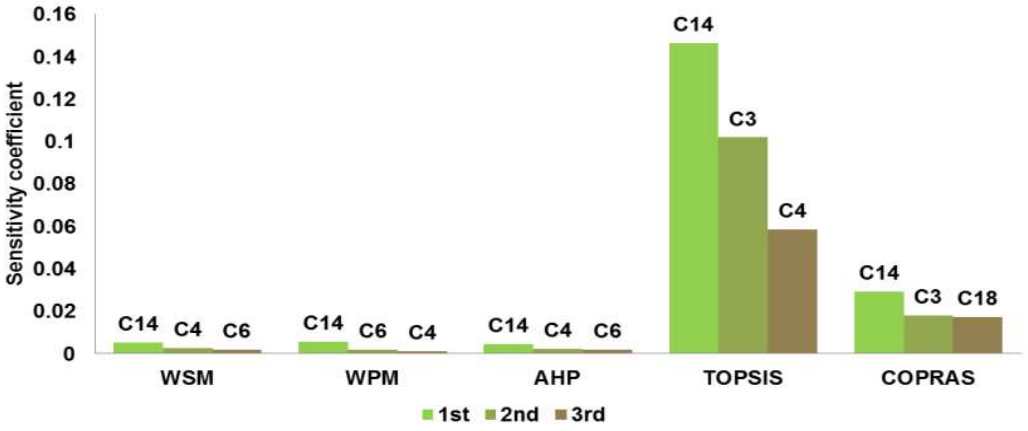
Using multi-criteria decision-making (MCDM) methods, it is possible to select the appropriate application development process from a group of contrasting and diverse processes. Because it can use specific criteria to evaluate various options, the MCDM is an excellent method for analysing complex real-world problems (Samantraj et al., 2020). In addition, the MCDM theory occupies a unique and significant position in science. Because MCDM methods are used to break down complex problems into smaller parts, all the parts will be put together after the analyses, giving a complete picture of the problem. When it comes to solving problems in more complex areas, the decision-making process necessitates the prior definition and fulfilment of factors.

The application of MCDM methods enables the decision-maker to consider a variety of criteria or objectives to reach a compromise between all the parameters that could be incompatible. As a result, decision-makers must take quantitative and qualitative factors into account and evaluate them. The criteria may be considered by the MCDM strategy alongside subjective and quantitative characteristics (Costa *et al.*, 2019). There are a lot of different criteria that can be looked at for different problems with selecting a manufacturing process. When there are several options, the following two factors must be considered when solving the problem of deciding (Tan et al., 2021). First and foremost, it includes planning about the various factors that affect the problem, such as manufacturing processes. The selection of the best MCDM strategy for the issue at hand is the second factor. It is a well-known fact that the performance and characteristics of various MCDM methods vary. As a result, selecting a particular MCDM strategy from the available options is challenging. In most

cases, to increase selection efficiency and effectiveness, a comparative evaluation of various MCDM techniques is required.

An example of the evaluation that has been widely considered in most studies is the sensitivity of the models (Costa *et al.*, 2019). Each of the models has been subjected to the presentation of the information and the handling of issues being subjected to the factors of decision making. In a comparative analysis on the applicability of the models, the AHP model was viewed as having the least sensitive approaches. The figure below portrays the sensitivity levels for each of the MCDM Models as determined by Maliene et al., (2018). This consideration is sufficient to consider the application in the selection of the important model for each industry. Based on Figure 6, the application of the AHP model connects the technology to the right model to derive the best decision in the process of making the right choice for security features for applications.

Figure 3:Sensitivity of the MCDM Models



Source: Maliene et al., (2018).

Another evaluation used to assess the applicability of the decisions is that of evaluating the computational complexities. This can be derived through assessing the connection between a decision model and the select complexity for that model (Karande & Joshi, 2022). A comparison done for three models indicated the following level of complexities for the decision models. The comparison was for AHP, TOPSIS, and VIKOR methods. The complexity for AHP was lower than TOPSIS but higher than VIKOR methods (Kabassi, 2022). Application of such complexities would be ideal in the moving technological advancements to higher levels.

The ELECTRE method falls in the middle of compensatory and non-compensatory approaches. Simply put, the trade-off is permitted to the extent that the decision-maker decides. The approach developed by ELECTRE is based on paired comparisons and makes use of an outranking relationship to rank, sort, and select the best option (Kabassi, 2022). Due to the inaccuracies of existing evaluators in the decision-making issues, this method offers the possibility of fitting various utility functions from various decision-makers and employing quasi-criteria rather than actual criteria (Han *et al.*, 2016). The ELECTRE method is more reliable than other methods that are sensitive to the beliefs of decision-makers because it can be used to compare alternatives even when there is no clear preference for one of them.

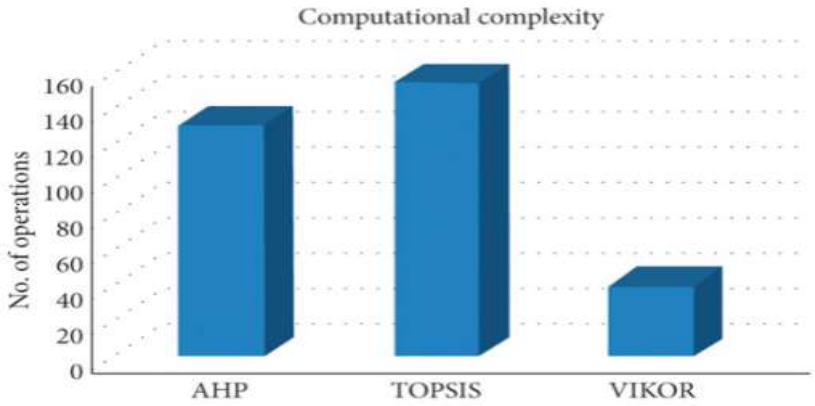
A crucial component of decision-making models for developers of mobile applications is compromise. This focuses on finding a solution that meets the needs of all parties and produces the best possible outcome. Mobile app developers can find the best options with the least amount of effort and resources by incorporating compromise into the decision-making process (Samantraj et al., 2020). This is especially crucial in the academic setting, where ethical decision-making and teamwork are critically important. Additionally, developers of mobile applications can analyze the likelihood of conflict and foster an atmosphere of mutual respect and cooperation by employing compromise (Khan, Khan & Pandey, 2021). Therefore, for mobile app developers to achieve the best results, it is essential to comprehend the fundamentals of compromise and apply them to decision-making models.

To guarantee the best results, decision making models for developers of mobile applications need to include a compromise option. According to Michael et al. (2019), the compromise makes it possible to consider a variety of points of view, which makes it possible to evaluate the various options in a more thorough and comprehensive manner. It makes it more likely to get the results you want and less likely to try to find a bad solution (Samantraj et al., 2020). In addition, developers can improve the overall efficiency of the decision-making process by reaching a compromise that is agreeable to all parties. As a result, successful and efficient mobile app development necessitates the inclusion of a compromise option in decision-making models for app developers.

A less complex computational approach like VIKOR method may not desirably present the appropriate decision model for the mobile technology developers noting that their security options must capture diverse data. The big data technologies being integrated into

the telephony sector mean that there is enhanced diversity of the information that is considered when enhancing the security measures in the applications (M. Venkata Krishna Reddy et al., 2022). As such, authors have desired to connect the decision models to come up with a combined or variegated application of the methodologies in defining the means through which the models can be more impactful. Some of the areas of studies have been on the elements of the decision-making models and how they can relate to each other. A study to assess the comparative complexities (see figure 6) in the computational methods used in dealing with the regard for decision-making models was conducted by Chen et al (2014)

Figure 4: Computational Complexities in MCDM Methods



Source: Chen et al., (2014)

The mobile application's network connection to the server may also be vulnerable to attack. Therefore, the obvious place to begin is to ensure the safety of communication. The app's code ought to be able to distinguish between legitimate security certifications and invalid requests. Developers have a role to play in preventing attackers from gaining unauthorised access by verifying the authenticity of security certificates (Han *et al.*, 2016). Before allowing employees to use them on mobile devices that connect to the corporate network, IT departments may also decide to vet mobile apps to ensure that they comply with security policies.

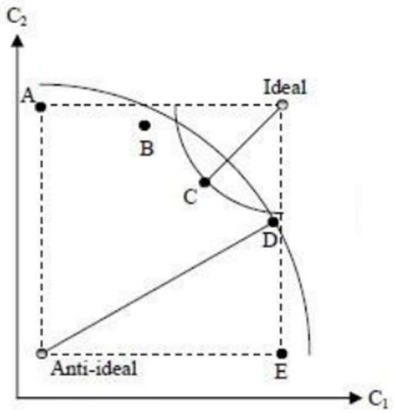
Due to the on-going discovery of new mobile device vulnerabilities, communicating mobile security threats and best practices has emerged as a central objective. Mobile applications have had to deal with a wide range of internal and external security threats over the past few years. In the context of organizational information security, decision-making is heavily

reliant on a variety of data (Han e*t al.*, 2016). Depending on the content and type of application, mobile applications differ in terms of security and performance.

4.6 TOPSIS

Another MCDM model that can be applicable in mobile security development is the TOPSIS model. TOPSIS stipulates that the closest alternative to the positive ideal solution (PIS) should be the best one. It must be as far away from the negative ideal solution (NIS) as possible. The normalized decision matrix (NDM) is the first of the various steps in the TOPSIS approach (Tan et al., 2021). The element normalized decision matrix and the NDM are utilized to express the generated DAs' relative performance. The weighted decision matrix, or WDM, is then calculated. A comparison matrix table indicates the criterion and alternatives as analysed by Maliene et al. (2018). The distance of separation for each option derived from PIS and NIS can be calculated with the assistance of a subsequent focus on the WDM-based definitions of PIS and NIS.

Figure 5:Two Criteria Graphical Representation



Source : (Waxler, J., 2018)

4.7 Analytic Hierarchy Process (AHP)

Considering the AHP model of dealing with installation of security features in the apps under each of the models can provide different results and these can be addressed differently (Tan

et al., 2021). The AHP is one of the most well-known methods for determining the relationship between design characteristics and customer requirements. A four-step process is used to put the AHP approach into action. The equation for a paired comparison matrix is first created. For a cluster with "n" customer demands, an overall number of pairwise comparisons equal to [n (n1)/2] must be evaluated. The various attributes, as well as their reciprocals, are evaluated using a 9-point Likert scale. Pairwise comparisons were used with AHP to quantify the preference degree of decision makers and stakeholders regarding the manufacturing process of choice.

The normalization of the geometric mean (NGM) method is used to calculate the attributes' relative importance. According to Song *et al.* (2018), the consistency in the degree of importance that is determined for the characteristics assesses the appropriateness in the decisions that ought to be taken regarding a given technical issue. It is abundantly clear that the accuracy of the chosen material is the user's top priority. A consistency test is necessary to ensure that pairwise comparison is appropriate and rational. Adequacy to changes in alternatives or criteria, adaptability during the decision-making process, computational complexity, and support for group decision-making, the number of alternative manufacturing processes and criteria, and uncertainty modelling are all factors to consider (Costa *et al.*, 2019). A look at the application of each of the MCDM procedure can prove the relevance and ability to handle the matters that are considered as important to the mobile app developers (Strzelecki, 2020). Even though pressure reduction is addressed during the mobile generation, in terms of shedding most weight of the operation cost, AHP is still the best decision-making model for the mobile phone manufacturing or development process (Yasumatsu *et al.*, 2019). Such is in terms of the overall evaluation out of all the competing application development processes.

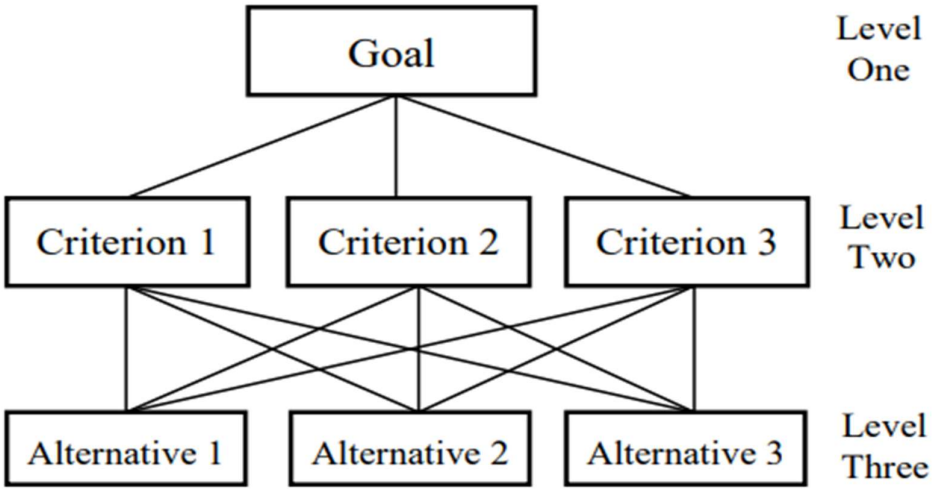
4.7.1 Steps of AHP:

Step 1: Model development and step formulation

The problem and objective of the decision-making process are introduced hierarchically into the context of the relevant choice factors in the first stage. Decision indicators and decisions are components of the decision-making process. A hierarchy was developed by the group.

Determining the purpose, criteria, sub-criteria, and alternative and then organising them into a hierarchical framework is called decision modelling.

Figure 6: AHP decision model



Source: own work

Step 2: Pairwise Comparison and Attribute Weighting

In the second step, the weights of the criteria must be decided. By evaluating the criteria in pairs with respect to the goal and the decision issue, weights are established. This method uses pairwise comparison to create a ratio matrix. The decision-maker can be asked a variety of questions, such as "Which of these two attributes is considered more important, and how significantly more important?" to compare the relevance of two variables at once. In the AHP, the Saaty's nine-point scale is used for comparisons.

Table 3: Saaty's pairwise comparison scale

Verbal Judgement	Numerical Value	Description
Equal Importance	1	Two choices contribute equally to objective

Moderate Importance	3	One choice slightly favors over another
Strong	5	One choice strongly favors over another.
Very strong Importance	7	One choice is very strongly favored over another
Absolutely strong Importance	9	One choice is most important over another.
Middle ground values	2, 4, 6, 8	Represents intermediate values.

Source: (l. Saaty,1977)

A (M x N) evaluation matrix A can be used to summarise the results of the pairwise comparison of n criteria. Each member aij in the matrix expresses the relative importance of the criterion in row I to the criterion in column j.

$$A = \begin{bmatrix} 1 & a12 & a13 & \dots & a1N \\ a21 & 1 & a23 & \dots & a2N \\ a31 & a32 & 1 & \dots & a3N \\ \dots & \dots & \dots & \dots & \dots \\ aM1 & aM2 & aM3 & aM4 & aMN \end{bmatrix}$$

Fig: Evaluation matrix

From the above matrix

$$a_{ji} = \frac{1}{a_{ij}}$$ ……Equation 1

$$a_{ij} \neq 0$$

Table 4:Pairwise Comparison Table

	Criteria 1(C1)	**Criteria 2(C2)**	**Criteria 3(C3)**	**Criteria 4(C4)**

Criteria 1(C1)	C1 Agnaist C1	C1 Against C2	C1 Against C3	C1 Against C4
Criteria 2(C2)	C2 Against C1	C2 Against C2	C2 Against C3	C2 Against C4
Criteria 3(C3)	C3 Against C1	C3 Against C2	C3 Against C3	C3 Against C4
Criteria 4(C4)	C4 Against C1	C4 Against C2	C4 Against C3	C4 Against C4

Source: Own work

The resulting matrix A must be reciprocal to meet a basic consistency need; otherwise, the decision-maker might have misunderstood the situation. Since the members of the matrix's major diagonal represent the circumstance in which a criterion is compared to itself, it is also evident that every member has a value of 1.

Relative weights (v) of the criterion can be computed from the generated matrix by means of the normalised Perron-Frobenius eigenvector The resulting matrix A must be reciprocal to meet a basic consistency need; otherwise, the decision-maker might have misunderstood the situation. Since the members of the matrix's major diagonal represent the circumstance in which a criterion is compared to itself, it is also evident that every member has a value of 1.

Relative weights (v) of the criterion can be computed from the generated matrix by means of the normalised Perron-Frobenius eigenvector. Consequently, all the criteria weights added together will equal one. The only idea that has a direct impact on the AHP's output level is consistency. Consequently, all the criteria weights added together will equal one. The only idea that has a direct impact on the AHP's output level is consistency.

$$a_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \quad \text{.....Equation 2}$$

Next, the values for each row are averaged to get the criterion weight.

$$Cw_{ij} = \frac{\sum_{i=1}^{n} a_{ij}}{n}$$ .....Equation 3

Step 3 Consistency ratio

As was said in the part above, consistency rates how well the AHP produces results. Stated differently, consistency guarantees that judgements be made without logical contradictions. Some consistency in the AHP is imposed by mandating that matrix A be reciprocal (Saaty, 1971). Explicit transitivity may not always be demonstrated despite this. For example, it is important to verify that, in addition to favouring alternative 'b' over alternative 'a,' a random decision maker also favours alternative 'a' over alternative 'c'. Although this makes mathematical sense, irrational conduct usually has an impact on decision-makers.

This produces inconsistent and biased outcomes. In addition to following the logical foundation of the preferences, consistency necessitates the cautious use of precise assessments of preference intensity, as the use of excessive.

$$CI = \frac{\lambda max - n}{n-1}$$ .....Equation 4

N, the total amount of choices for totally reciprocal and reflexive comparison matrices (or criteria), should equal the greatest eigenvalue of matrix A. High CI levels, on the other hand, suggest a problem. Low CI values often show minimal inconsistency. Saaty defined the allowable value of (in)consistency and provided a formula for calculating consistency ratio (CR), which compares the CI of the in-question matrix with the consistency index of a random-like matrix (Saaty, 1971).

Table 5: Saaty's Radom Index

n		2	3	4	5	6	7	8	9	10

RI		0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Source: (Saaty, 1971).

The consistency ratio is defined as

$$CR = \frac{CI}{RI}$$.....Equation 5

When the appropriate consistency ratio is 0.10 or below, the AHP analysis can be considered to have produced consistent results, according to Saaty (Saaty, 1971). When the CR exceeds 0.10, The review procedure must be repeated to identify and deal with the inconsistent source.

Final Priority

The objective of this stage is to determine the relative weights and overall priority of the alternatives with respect to each criterion separately. The method is the same as in the previous stage; it involves comparing each choice in pairs according to each criterion. As previously, a consistency check is required. After accounting for the importance of each criterion, the weighted total of all the determined alternative priorities is added to ascertain the overall priorities of the alternatives. The optimal choice is the one that has the highest overall importance. Sensitivity analysis is also necessary to comprehend the logic underlying the given results. To ascertain the possible impacts of altering the criterion weights on the outcome, research is conducted.

4.8 Fuzzy AHP

In making decisions, fuzzy AHP tackles the drawbacks of sharp values. Although decision-makers in classical AHP assign exact values to pairwise comparisons between criteria and options, uncertainties and imprecisions may occur in real-world situations. Decision-makers

may express preferences in a more flexible and realistic way thanks to fuzzy logic, which fuzzy AHP adds to capture and represent these uncertainties. It provides a more sophisticated approach to decision support in complex systems by including fuzzy numbers and linguistic variables to represent the imprecise nature of human judgements.

4.9 Weighted Sum Model (WSM)

The WSM also known as SAW, Formula is a model in which: The best alternative's WSM score is A WSM-score, the number of decision criteria is n, the actual value of the I^{th} alternative in relation to the J^{th} criterion is a_{ij}, and the weight of importance of the J^{th} criterion is W_j. It is critical to point out here that WSM only applies when all data are expressed in the same unit. Based on this evaluation, the maximum of importance is weighted against the averages and weights of each item.

Cw_{ij} can be used to put the WSM normalisation approach for benefit and cost criteria into practise, making sure that the final decision goal makes sense.
The following formula is used to standardise WSM during the normalisation procedure:

$$\mathbf{a_{ij}} = \frac{\mathbf{x_{ij}}}{\sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{x_{ij}}} \quad \text{……Equation 6}$$

When criteria have multiple dimensions or various units, their values are adjusted. These could be cost or benefit-related criteria.
The formula is used to calculate the values of the positive criteria.

$$a_{ij} = \frac{x_{ij} - D_j}{|H_j - D_j|} \quad \text{……. Equation 7}$$

The formula is used to calculate the values of the Negative criteria.

$$a_{ij} = \frac{x_{ij} - D_j}{|D_j - H_j|} \quad \text{……Equation 8}$$

This is the exact amount of the difference that is utilised between the criteria's highest value (Hi) and its smallest value (Di).

is the normalised performance rating, and each criterion's attribute value is represented by Xij. is each criterion's maximum value and is each criterion's lowest value.

Benefit occurs when the value is at its highest, while cost occurs when the value is at its lowest.

is the alternatives Ai's normalised performance rating on attribute Cj. (i=1, 2..., m) and (j=1, 2..., n)

Each alternative's preference value (Vi) is provided as follows:

$$u(a_i) =\ldots \quad \sum_{j=1}^{k} v_j a_{ij} \quad \text{.....Equation 9}$$

Where $u(a_i)$ is the ranking for each alternative Vj is the weighted value of each criterion, a_{ij} is the normalized performance rating value. A larger $u(a_i)$ value indicates that the alternative Ai is preferred.

5 Practical Part

5.1 Description of problem

Following an overview of the MCDM problem literature, each method's best practice implementation is shown to help stakeholders and decision-makers make decisions in real-world applications. Such applications are relative in regard for the app developers who are daily realizing new challenges emanating from the presence of new platforms within which applications must develop. Besides, the connection between application and the updates that are done on the phones and other gadgets remains very wide with new apps rising each day. Infringement of security concerns remains a major issue in dealing with the rising need to have resilient applications. Thus, the focus for the study is to establish the challenges and comparative relevance of the security considerations for the app safety by the app developers. There is consideration of competing criteria in uncertain environments which the app developers have to consider them. In this assessment the applicability of the right methodology when it comes to consideration of the security features in app development is reviewed. This is owing to the rising presence of predatory applications that tend to infringe on the resilience of other apps. The consideration of the MCDM methods is made based on the perceptions from the app developers and the realization of the most appropriate or closely relevant method considered.

There have been significant contributions in which various MCDM strategies have been proposed by researchers. However, the literature on manufacturing process selection rarely contains a methodology that can compare the various MCDM techniques. In the context of selecting a manufacturing process, additional comparative evaluations of various approaches are still required (Strzelecki, 2020). Developers of mobile applications need to consider a compromise variant as an alternative to creating an app that is fully functional. While avoiding the costs of creating a full-featured app, the compromise variant can give the developers the leeway to make the users access basic features while reducing the feature set.

The compromise variant in decision making process can evaluate the challenging but doable processes to over the obstacles for developers of mobile applications. Samantraj et al. (2020) explains that the development teams can find the best solution that both meet their project's specific requirements and the constraints of limited resources, capabilities, and

other related factors with careful analysis. Developers of mobile applications can guarantee that the best outcomes are achieved by placing such an emphasis on achieving the appropriate balance and approach (Ksibi et al., 2022). Comparative methods analysis in the context of manufacturing process selection is also required to fill the gap between utility and technological advancement. As a result, this work develops a method for evaluating various decision-making strategies for mobile phone application makers who need to focus on extensive or useful security features.

5.1.1 Alternative Decision Models.

The alternatives in MCDM are the set or group of similar choices that seems important to achieve the goals. Alternatives differ from problem to problem. Sometimes it can be difficult to find the alternatives in such case we should create wish lists or have conversations and brainstorming sessions with people whose judgement and expertise we respect to spark our imagination and see several approaches to our choice. We have listed seven alternatives which can be best fit mobile application security measures.

1. Access Control (A1)
2. Data Protection (A2)
3. Application Security Testing (A3)
4. Vulnerability (A4)
5. App Shielding (A5)
6. Threat Modelling (A6)
7. Session Management (A7)

Access Control

Access control is a key element of data security, which establishes restrictions on who may access and utilize Users resources and information. The main component of access control are Authentication and authorization. Access control ensures that the user is genuine and has the right access data through permission and authentication. Limiting physical access to buildings, datacenters, rooms, and campuses is another purpose for access control. Access control verifies multiple login credentials, such as usernames and passwords, biometric scans, and other

security features to identify users. Multifactor authentication needs many authentication techniques to confirm a user's identity.

Data Protection:

Users' security and privacy of data is one of the main issues in today's digital world. The increasing frequency of cyberattacks and breaches has made data security management an essential component of mobile app development. Hackers are always experimenting with new methods and strategies to take advantage of holes in mobile application security. For your apps to function effectively, security must be enabled so that risks to your important data and assets are minimized. Applying security measures like data encryption and data masking involves several steps that make up data protection.

Application security testing

The process of evaluating, assessing, and reporting on an application's security level as it progresses through the software development life cycle is known as application security testing (AST). Through the identification of security flaws and vulnerabilities in the source code, AST increases the resistance of applications to security attacks. Automated, manual, dynamic, interactive, and a combination of both can be found in AST. Furthermore, most software applications that interface with operational technology (OT) or industrial control systems may be developed using the same AST approaches as are used for traditional IT applications. Data historians, control application software, and human-machine interface software are a few examples of these OT-related applications.

Vulnerabilities:

A vulnerability is a flaw in an information technology system that an attacker may use to launch a successful threat. Attackers will try to take advantage of any of these combining one or a greater extent to accomplish their ultimate objective. They can arise from weaknesses in security, functionalities, or user mistakes. All types of attackers aggressively seek and take advantage of vulnerabilities.

App shielding:

The key security feature that prevents access into the app is app shielding. Essentially, it shields user data and attack attempts from the negative effects of security breaches. Hackers find it more difficult to infiltrate and launch attacks when using app protection. It uses several strategies to stop attempts at code tampering and seal similar security flaws.

Threat Modelling:

The purpose of threat modelling is to protect valuable assets by recognizing, articulating, and comprehending risks and mitigation strategies. An organized depiction of all the data influencing an application's security is called a threat model. It is essentially a program and its environment seen via a security lens. Many different types of systems, networks, distributed systems, software, apps, and Internet of Things (IoT) devices may all benefit from the use of threat modelling.

Session Management:

The technique of securely managing several requests made by a single user or organization to a web-based application or service is known as session management. A session is a collection of HTTP requests and transactions started by the same user. Websites and browsers communicate via HTTP. When a user verifies their identity with a password or another authentication procedure, the session usually begins. Since exchanging secrets with authorized users is a part of session management, safe cryptographic network connections are necessary to keep session management secure.

5.1.2 Choosing Important Decision Criteria for Calculations

In applying the various criterions in handling the responses regarding the various aspects of handling decision making for mobile security development, there is consideration of the various attributes of security features adopted by the App developers in enhancing the security features. An initial collection of information from randomly selected respondents regarding the security features was conducted. The credit scores assigned to a particular subject are what is used to define criteria of analyzing the data.

In selecting the best security measures for mobile applications, we have considered seven criterions which are most important to a user to decide which security measure is best from the provided set of alternatives. The criteria are Security Impact (C1), Exploitation Time

(C2), Implementation Time (C3), Maintenance Time(C4), Effectiveness (C5), Adaptability (C6), Adverse Effect (C7).

Table 6:Decision criteria and decision units that are relevant.

Criteria	**Sub-Criteria**	**Code**	**Unit**	**Denoted by**
Security	Security Impact	S. I	%	C1
Time	Exploitation Time (using time)	Ex. T	Months	C2
Time	Implementation Time	I.T	Months	C3
Time	Maintenance Time	M.T	Months	C4
Effectivity	Effectiveness	EF	%	C5
Time	Adaptability time (how fast the security system can be modified)	A. T	Months	C6
Effects	Adverse Effects	A. E	%	C7

Source:own work

5.2 Research Process and Data Collection

This study conducted by first gathering secondary information regarding the MCDM models. Resources were screened from the categories of journals, conference papers, peer-reviewed articles, and books. These resources laid the basis of conducting further evaluation using the primary assessment of the opinions based on assessment of the various models that are used in decision making. The study culminated in the evaluation of resources, especially the one evaluated from OECD platform. Besides, an assessment of the merits and demerits

of the MCDM approaches is conducted with the opinions evaluated from the app developers' perspective.

Scoring a criterion for security impact often benefits from the use of objective data, with the most effective methods involving the assessment of known attacks. This process includes evaluating the security impact of each attack, linking them to the specific controls capable of preventing them, and then generating a comprehensive score for each control. However, obtaining such data is currently unavailable and poses significant difficulties in terms of production. The data is taken from the research paper that used Expert Elicitation (EE) method out of 25 people and also data are taken from crossref it is a platform which provides users data for research purposes.

According to Slottje et al. (2008), "Expert elicitation refers to a systematic approach to synthesize subjective judgments of experts on a subject where there is uncertainty due to insufficient data, when such data is unattainable because of physical constraints or lack of resources."

Table 7:Corresponding data with criteria and alternatives for the study

	Criteria	C1	C2	C3	C4	C5	C6	C7
Alternatives								
A1		2.53	2.93	2.13	1.6	2.2	2.80	1.21
A2		1.93	2.8	1.67	1.33	1.73	1.6	3.2
A3		2.73	2.6	2.53	1.87	2.2	2.32	2.87
A4		2.07	2.8	2.87	1.73	1.6	1.03	1.76
A5		2.4	3.27	3.2	2.07	1.6	3.2	2.22
A6		2.2	3.53	3.33	2.67	1.53	1.30	2.87
A7		2.27	3.8	3.2	2.73	1.93	1.67	3.92

DataSource:https://www.proquest.com/docview/2030547071?pq-origsite=gscholar&fromopenview=true

https://search.crossref.org/

5.2.1 Selecting an Approach to Determine the Compromise Variant

Once the choice problem was framed, a multicriteria approach was required to assess the alternative's broad impact in relation to the established criteria. The concepts of Weighted Sum Model (WSM) and the Analytical Hierarchy Process (AHP) were utilised. The weight of the chosen criterion was determined using AHP, and the variation was ranked using WSM. Because it helps decision-makers convert subjective evaluations into objective measurements, AHP is important as it offers a pairwise comparison approach to further define the relative relevance of the performance criteria and provide significant weightings to them.

5.2.2 Evaluations of MCDM Approaches

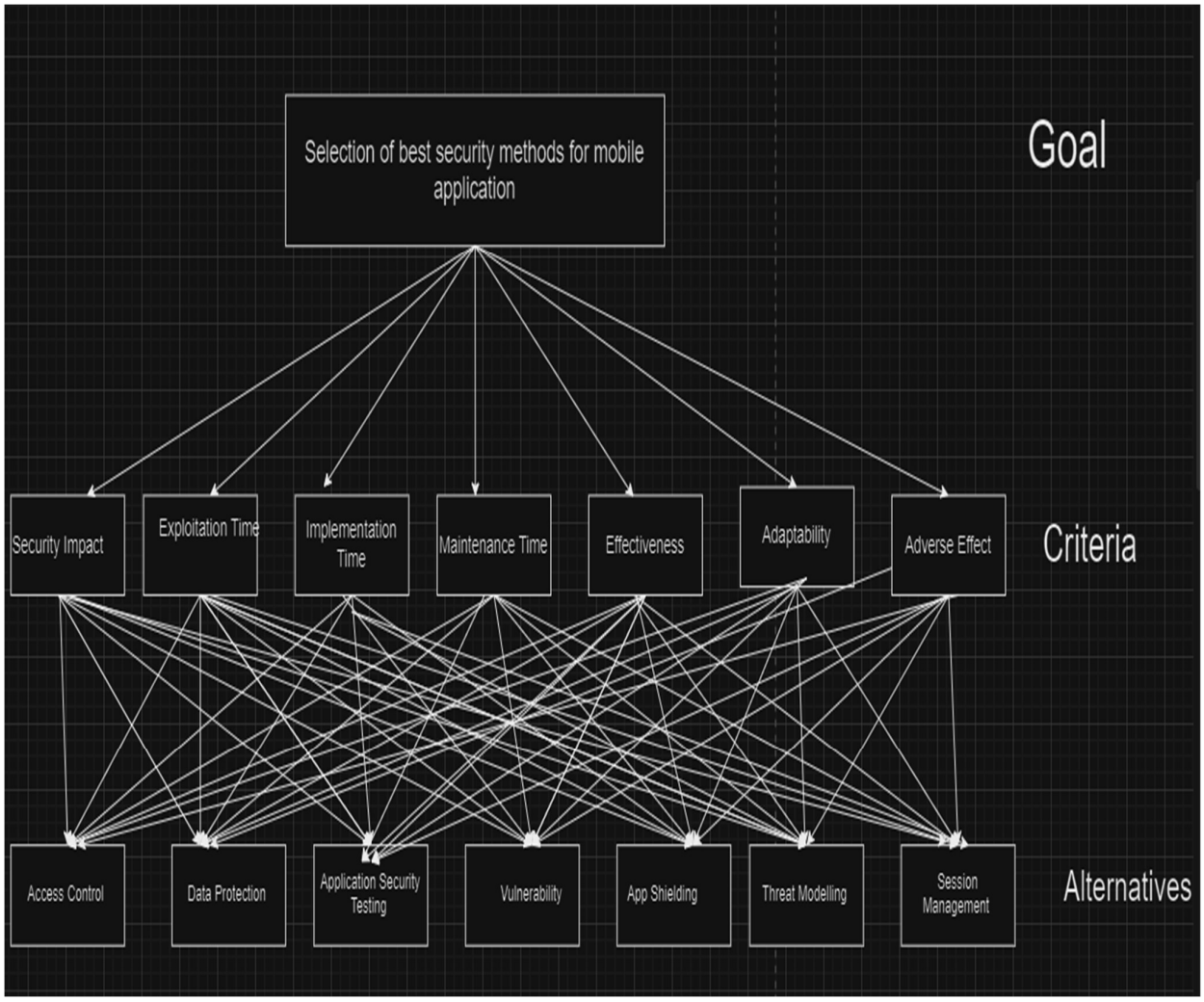
In applying the various criterions in handling the responses regarding the various aspects of handling decision making for mobile security development, there is consideration of the various attributes of security features adopted by the App developers in enhancing the security features. An initial collection of information from randomly selected respondents regarding the security features was conducted. The credit scores assigned to a particular subject are what is used to define criteria of analyzing the data.

5.2.3 AHP Model development and problem formulation:

With the help of a consultant with extensive knowledge of app development and mobile application security, as well as research of the literature, all quantitative factors influencing the decision-making process were identified. The following considerations were used while performing this Security Impact, Exploitation Time, Implementation Time, Maintenance Time, Effectiveness, Adaptability, and Adverse Effect.

A hierarchical structure based on the objective, criteria, sub-criteria, and options was created using the information that was gathered. An assessment model with seven primary criteria is created, as seen in the figure below.

Figure 7:Decision hierarchy for choosing a Security Methods for mobile applications



Source :Own work

5.2.4 Pairwise ComparisonMatrix

After constructing the hierarchical structure, a pairwise comparison of the decision-making criteria was done. The findings are shown in the following table. Every cell in the comparison matrix will represent our relative preference for each of the examined pairs and

have a value from the numerical scale shown from Saaty's pairwise comparison scale. This was done with advisers and specialists' assistance.

Table 8: Pairwise Comparision Matrix

	C1	C2	C3	C4	C5	C6	C7
Security Impact (C1)	1	3	3	5	5	5	5
Exploitation Time (C2)	0.33	1	3	3	3	3	3
Implementation Time (C3)	0.33	0.33	1	3	5	7	7
Maintainance Time(C4)	0.2	0.33	0.33	1	3	5	3
Effectiveness (C5)	0.2	0.33	0.2	0.33	1	2	3
Adaptability (C6)	0.2	0.33	0.14	0.2	0.5	1	3
Adverse Effect (C7)	0.2	0.33	0.14	0.33	0.33	0.33	1
TOTAL	**2.46**	**5.65**	**7.81**	**12.86**	**17.83**	**23.33**	**25**

Step 1: Normalizing the data.

The collected data regarding the aspects of security that are considered in the evaluation of the App developers' options in dealing with security features is provided. This involves the consideration of the averages from the responses garnered regarding the developers' concern over the aspects of the apps that need enhanced features. Normalization considers each of the aspects and averages.

Table 9: Normalized Decision Matrix and Criteria Weights

	C1	C2	C3	C4	C5	C6	C7
Security Impact (C1)	0.4065041	0.530973	0.3841229	0.388802488	0.280426	0.214316	0.2
Exploitation Time (C2)	0.1341463	0.176991	0.3841229	0.233281493	0.168256	0.12859	0.12
Implementation Time (C3)	0.1341463	0.058407	0.128041	0.233281493	0.280426	0.300043	0.28
Maintainance Time(C4)	0.0813008	0.058407	0.0422535	0.077760498	0.168256	0.214316	0.12
Effectiveness (C5)	0.0813008	0.058407	0.0256082	0.025660964	0.056085	0.085727	0.12
Adaptability (C6)	0.0813008	0.058407	0.0179257	0.0155521	0.028043	0.042863	0.12
Adverse Effect (C7)	0.0813008	0.058407	0.0179257	0.025660964	0.018508	0.014145	0.04
TOTAL	1	1	1	1	1	1	1

Source: Own work

In the above table, there is the consideration of the mean correlation of factors that determine the app development. The use normalization procedure is used to calculate the criteria weight and alternative local weight that are selected from existing matrices. The following is an explanation of the equations for criteria weight and alternatives local weight. First, there is calculation of the weight for each row. It is calculated using this formula where the values for each row are averaged based on noted attributes.

$$Wi=\sum_{j=1}^{n} aij,\ i=1,2\ldots.n$$

Each of the weighted average is then normalized into the figures above based on the following formulae. In this step the weighted average cumulative is considered under the item and also per row. This gives a better reflection of the item and comparative for the various aspects being considered.

$$Wi = \sum_{j=1}^{n} aiJ \quad i=1,2\ldots n \quad \text{.....Equation 10}$$

$$/ \sum_{k=1}^{n} \sum_{j=1}^{n} akj$$

The figures are then considered under the Eigen vector (a) and then the weight vector (b) for an ultimate ranking.

a. $W^i = \frac{1}{n} + (A1+A2+A3\ldots+An$

The weighted average is evaluated on how the same meets the Eigen vectors criteria. The value of W^i is thus the summation of the n^{th} part of each of the averages.

b. $W = [W^1, W^2 \ldots\ldots W^n]T$

These weighted averages are then ranked based on the consideration of the values and hence they are used to derive the significance of the methodology in providing an ultimate decision for the mobile app development choices.

The mean for security feature consideration is based on the responses evaluated. The correlation between the consideration for security features and that of engaging in user-friendly factors in applications is 1 with the correlation between security features and team specialty being 5. For a better consideration on each of the factors contributory aspect to the other factor for the holistic integration of desirable feature in the apps, the contributory means is considered for each of the factors.

The total for each of the column is equivalent to 1 depicting that the means for each correlation leads to the total sum for each of the factors was significant and added to whole figure. However, there is need to consider the mean for each of the factors on the horizontal row. This consideration helps in the prioritization of the factors. The prioritization is as follows.

Step 2: Taking the Geometric Mean of each Row.

Table 10: Means for each of the multi-factor's considerations.

	C1	C2	C3	C4	C5	C6	C7	Mean	CW
Security Impact (C1)	0.4065041	0.530973	0.3841229	0.388802488	0.280426	0.214316	0.2	2.405146	0.343592
Exploitation Time (C2)	0.1341463	0.176991	0.3841229	0.233281493	0.168256	0.12859	0.12	1.345387	0.192198
Implementation Time (C3)	0.1341463	0.058407	0.128041	0.233281493	0.280426	0.300043	0.28	1.414345	0.202049
Maintainance Time(C4)	0.0813008	0.058407	0.0422535	0.077760498	0.168256	0.214316	0.12	0.762294	0.108899
Effectiveness (C5)	0.0813008	0.058407	0.0256082	0.025660964	0.056085	0.085727	0.12	0.452789	0.064684
Adaptability (C6)	0.0813008	0.058407	0.0179257	0.0155521	0.028043	0.042863	0.12	0.364092	0.052013
Adverse Effect (C7)	0.0813008	0.058407	0.0179257	0.025660964	0.018508	0.014145	0.04	0.255948	0.036564
TOTAL	1	1	1	1	1	1	1	7	1
		Table 3:Consistency Evaluation Table							

Source: Own Work

This leads to a prioritization consideration under the AHP evaluation based on the factors of security development considerations for Applications can be prioritized in the below expressed chart. Each row average is used to rate the ranking for each of the factors. Though the comparative variance between the considerations on the vertical and horizontal integrations may differ, the ranking helps in attaining a better regard for the significance of each of the aspect in the ultimate consideration of apps.

Criteria weight (CW)	0.344	0.192	0.202	0.109	0.065	0.052	0.037
	C1	C2	C3	C4	C5	C6	C7
Security Impact (C1)	1	3	3	5	5	5	5
Exploitation Time (C2)	0.33	1	3	3	3	3	3
Implementation Time (C3)	0.33	0.33	1	3	5	7	7
Maintainance Time(C4)	0.2	0.33	0.33	1	3	5	3
Effectiveness (C5)	0.2	0.33	0.2	0.33	1	2	3
Adaptability (C6)	0.2	0.33	0.14	0.2	0.5	1	3
Adverse Effect (C7)	0.2	0.33	0.14	0.33	0.33	0.33	1
TOTAL	**2.46**	**5.65**	**7.81**	**12.86**	**17.83**	**23.33**	**25**

Source; Own work

Based on the ultimate results, the ultimate evaluation portrays that the security features adoption is of higher ranking in terms of determining the security components integrated into apps. Figure above shows that the security features consideration supersedes the value given to the apps in terms of applying features. Therefore, during the allocation of resources for the handling of app security development features, the team will have the resources deployed under the below hierarchy distribution perspective.

n		2	3	4	5	6	7	8	9	10
RI		0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Fig: Saaty's Radom Index

Table 11:Calculation of : Consistency ratio

	C1	C2	C3	C4	C5	C6	C7	WSUM	CW	WSUM/CW
Security Impact (C1)	0.344	0.577	0.606	0.544	0.323	0.260	0.183	2.837	0.344	8.257
Exploitation Time (C2)	0.113	0.192	0.606	0.327	0.194	0.156	0.110	1.698	0.192	8.836
Implementation Time (C3)	0.113	0.063	0.202	0.327	0.323	0.364	0.256	1.649	0.202	8.161
Maintainance Time(C4)	0.069	0.063	0.067	0.109	0.194	0.260	0.110	0.872	0.109	8.003
Effectiveness (C5)	0.069	0.063	0.040	0.036	0.065	0.104	0.110	0.487	0.065	7.527
Adaptability (C6)	0.069	0.063	0.028	0.022	0.032	0.052	0.110	0.376	0.052	7.234
Adverse Effect (C7)	0.069	0.063	0.028	0.036	0.021	0.017	0.037	0.271	0.037	7.424
										55.442
			Lamda max =		55.442/7					
					7.92					
			RI = 1.32							
			CI=Lamda max-n/n-1							
			7.92-7/7-1							
			0.92/6							
		CI =	**0.153**							
		CR=CI/RI								
		CR=0.153/1.32								
		CR = 0.115								
		CR = 0.1								

Based on pairwise comparison table above the consistency ratio was calculated and the result was 0.1 which is less than 0.8 which means the pairwise comparison matrix is consistent.

Table 12:Criteria Weight from Normalized matrix

Criteria	**Criteria Weight**
Security Impact (C1)	0.343592215
Exploitation Time (C2)	0.192198207
Implementation Time(C3)	0.202049285
Maintainance Time(C4)	0.108899142
Effectiveness (C5)	0.064684119
Adaptability (C6)	0.052013088
Adverse Effect (C7)	0.036563943

From above table we can find that more priority is given to Security impact(C1) followed by Implementation time(C3) and adverse effect(C7) have minimum weight.

Using WSM approach to Rank the alternatives:

	Criteria weight	0.343592215	0.192198207	0.202049285	0.108899142	0.064684119	0.052013088	0.036563943
	Criterian feature	Possitive	Negative	Negative	Negative	Possitive	Possitive	Negative
	Alternatives\Criterian	C1	C2	C3	C4	C5	C6	C7
	A1	2.53	2.93	2.13	1.6	2.2	2.8	1.21
	A2	1.93	2.8	1.67	1.33	1.73	1.6	3.2
	A3	2.73	2.6	2.53	1.87	2.2	2.32	2.87
	A4	2.07	2.8	2.87	1.73	1.6	1.03	1.76
	A5	2.4	3.27	3.2	2.07	1.6	3.2	2.22
	A6	2.2	3.53	3.33	2.67	1.53	1.3	2.87
	A7	2.27	3.8	3.2	2.73	1.93	1.67	3.92
Basal Variant	**D**	1.93	2.6	1.67	1.33	1.53	1.03	1.76
Ideal Variant	**H**	2.73	3.8	3.33	2.73	2.2	3.2	3.92
Difference	|Hj-Dj|	0.8	1.2	1.66	1.4	0.67	2.17	2.16
	|Dj-Hj|	-0.8	-1.2	-1.66	-1.4	-0.67	-2.17	-2.16

Normalizing the matrix:

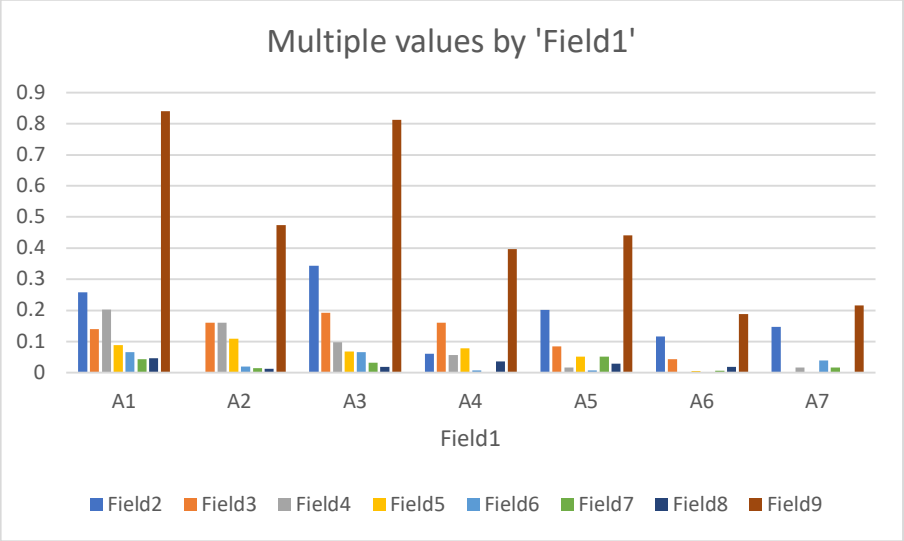
Criterian feature	Possitive	Negative	Negative	Negative	Possitive	Possitive	Negative
Alternatives\Criterian	C1	C2	C3	C4	C5	C6	C7
A1	0.75	0.725	1	0.807142857	1	0.815668203	1.25462963
A2	0	0.833333333	0.722891566	1	0.298507463	0.262672811	0.333333333
A3	1	1	0.481927711	0.614285714	1	0.594470046	0.486111111
A4	0.175	0.833333333	0.277108434	0.714285714	0.104477612	0	1
A5	0.5875	0.441666667	0.078313253	0.471428571	0.104477612	1	0.787037037
A6	0.3375	0.225	0	0.042857143	0	0.124423963	0.486111111
A7	0.425	0	0.078313253	0	0.597014925	0.294930876	0

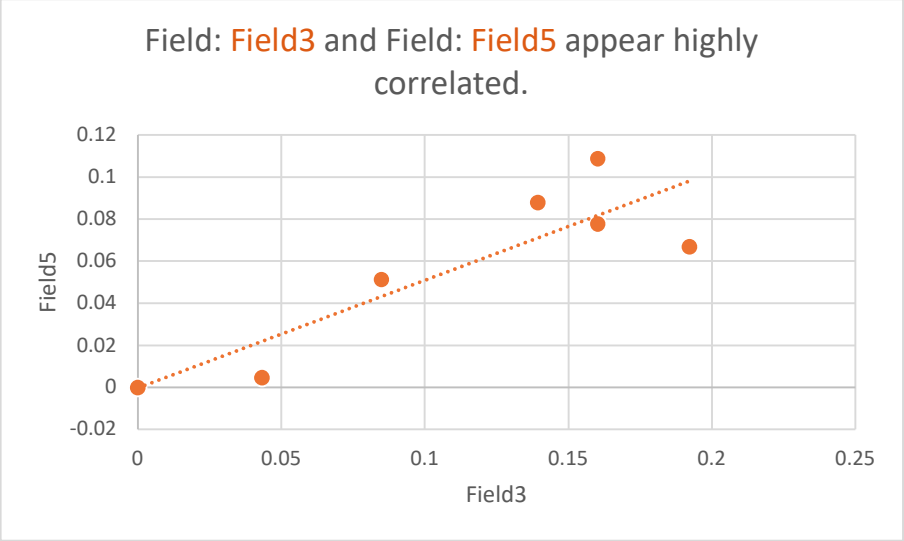
Multiplying each value by its respective criteria weight:

Criteria weight	0.343592215	0.192198207	0.202049285	0.108899142	0.064684119	0.052013088	0.036563943
Criterian feature	Possitive	Negative	Negative	Negative	Possitive	Possitive	Negative
Alternatives\Criterian	C1	C2	C3	C4	C5	C6	C7
A1	0.75	0.725	1	0.807142857	1	0.815668203	1.25462963
A2	0	0.833333333	0.722891566	1	0.298507463	0.262672811	0.333333333
A3	1	1	0.481927711	0.614285714	1	0.594470046	0.486111111
A4	0.175	0.833333333	0.277108434	0.714285714	0.104477612	0	1
A5	0.5875	0.441666667	0.078313253	0.471428571	0.104477612	1	0.787037037
A6	0.3375	0.225	0	0.042857143	0	0.124423963	0.486111111
A7	0.425	0	0.078313253	0	0.597014925	0.294930876	0

Ranking the alternatives:

Criterian feature	Possitive	Negative	Negative	Negative	Possitive	Possitive	Negative	Overall Result	Rank
Alternatives\Criterian	C1	C2	C3	C4	C5	C6	C7		
A1	0.257694161	0.1393437	0.202049285	0.087897164	0.064684119	0.042425422	0.045874207	0.839968059	1
A2	0	0.160165173	0.160165173	0.108899142	0.019308692	0.013662424	0.012187981	0.474388585	3
A3	0.343592215	0.192198207	0.09737315	0.066895187	0.064684119	0.030920223	0.017774139	0.81343724	2
A4	0.060128638	0.160165173	0.055989561	0.077785101	0.006758042	0	0.036563943	0.397390458	
A5	0.201860426	0.084887542	0.015823137	0.051338167	0.006758042	0.052013088	0.028777178	0.44145758	
A6	0.115962372	0.043244597	0	0.004667106	0	0.006471675	0.017774139	0.188119889	
A7	0.146026691	0	0.015823137	0	0.038617385	0.015340266	0	0.215807478	





In addition, the engagement of two or more MCDM models ensures a strategy to serve as a foundation for additional research into the creation of mobile applications' security development. According to Daradkeh & Sabbahein, (2019) the app development models lead to advances in existing approaches and can be utilized to achieve the desired result and have distinct benefits and drawbacks. However, it is essential to consider that after the engagement of the combined modes of the decision models, these strategies should not be used separately but rather in conjunction with one another to achieve the highest level of security throughout the development stages (Borissova, 2021). Besides, they still accommodate user preferences and convenience when considering the security features. These methods can be used to create a safe and reliable environment for mobile applications development with both consideration and compromise on select factors.

To uncover the content already discussing the MCDM approaches in considering and to assess the compromise variant in the application of the models, the secondary selection of the resources was conducted. The assessment sought to analyse the information in the resources available. An initial search by date was done but a subsequent analysis through relevance was initiated. The exercise was conducted severally to establish a basis of having each of the sought for content addressed. Besides, the evaluation was to help in uncovering the terms of discussing the various contents in the resources based on descriptions. The results of the studies were also evaluated in terms of how the models dealt with the challenges of the applied section.

The analytical aspects of the models were then assessed on the implications they have in terms of compromise variant. A check on the publication year and the relevance of the content in the resource was used to highlight the aspects that are needed for the study. Choosing from a variety of sectors is like deciphering a multi-variable, complex problem in a variety of conditions and dimensions with probably incorrect information. Every decision-maker is under the impression that making a bad decision or making a mistake during the problem-solving process will undoubtedly result in the system's failure and encourage poor management practices (Suomalainen *et al.*, 2022). Poorly managed decision-making formulations that have a significant impact on the organization's future and propagate a negative social image in the community are the consequences of disrupting such a system. Each of the resources content was used for the discussion in this study.

6 Future Models of Decision Making for Application Security Development

Innovative IT products should be developed with the interests and requirements of all important stakeholders in mind. Proposed use of computational approaches in developing applications and the description of the MCDM models will continue to advance in the mode of considering the application security (Zaidi et al., 2022). Technology advancement makes it possible to create formal models that match the need and demands for the theorized applications. According to Teymourzadeh et al. (2017), the heuristic algorithm with optimisation function is provided for MCDM modelling and testing the provided models. Tools are needed to help application security teams to take up the adopted programming choices to make the apps better and resilient.

To assess the robustness of each MCDM model and ensure that the results produced by each model are consistent, a sensitivity analysis is carried out. Using a different weighting scheme and recalculating the final value for each alternative website using each of the MCDM models is how the sensitivity analysis is carried out. AHP has a formal way to estimate weights and support criteria hierarchies, like the one in the current experiment. AHP claims that a group of evaluators comprised of domain specialists and software engineers was established (Wu, 2022). For pair-wise comparisons of the dimensions and pair-wise comparisons of the criteria for each dimension, each expert was required to complete three matrices. The values and rankings of each MCDM model calculated using the two distinct approaches are then contrasted. The Pearson correlation coefficient is used to compare the values of each model using various weighting schemes, and the correlation between rankings is checked during the comparison (Zaidi et al. 2022). In order to solve the problem of making a decision, PROMETHEE II sets up a complete pre-order on the list of websites that could be suggested to the decision-maker.

When qualitative criteria like the effects on the environment or politics are considered, the AHP is especially important. Due to its simplicity and consistency-checking capabilities, it is widely used for energy planning issues. Besides, all through this technique, the ordered progression is uncovered after the breakdown of the issue, which empowers understanding and characterizing the actual cycle (Khan et al., 2021). It is additionally appropriate for managing mechanical qualities and future perspectives that are not notable. It is important to note that AHP does not perform well when different levels are independent, so it cannot directly consider potential associations between many components. This

indicates that the method does not accurately represent the intricate connections between the components. The ANP method, for example, is one of the proposed AHP method extensions that can address these issues.

There has been generality in the consideration of MCDM models for producing disparate outcomes and no model has proven to be superior across all domains. A general framework for implementing and comparing MCDM models for the evaluation of application in generation of websites and various fields has previously been a key focus for researchers (Khan et al., 2021). In order to put the MCDM models into practice and compare them, the generalized framework provides the steps and specifics necessary for their implementation. The paper has noted that researchers stand to gain from the pre-existing information but still need to develop further studies on the information because it will make it simpler for the technicians to resolve security matters and decisions. There was significant evaluation on how studies have expressed how MCDM models apply and compare the models for use in compromise variant analysis.

As a means of back-end synchronisation of the data developed to deal with the arising matters, the teams must be focused on advancing their concentration on the factors that affect development of security features in applications. According to Teymourzadeh et al. (2017), security measures should be in place on the servers from which that mobile app accesses data to prevent unauthorized users from doing so. Back-end services must be strengthened against malicious attackers. This means that all APIs should be checked and secured appropriately to ensure that only authorized personnel can access them (Teymourzadeh et al., 2017). They must constantly evaluate and monitor an application's security posture. The combination of security knowledge at all application levels is referred to as security posture. More artificial intelligence will be used because the human analyst will not be able to process all the information (Tao et al., 2020). Security teams must prioritize and create a backlog of issues to address based on this information. Businesses must not only address security in the present but also anticipate and prepare for security threats posed by future technologies as the internet becomes increasingly important to millions of people worldwide (Wu, 2022). Predictions of the future may seem fancy and catch people's attention, but when it comes to cyber-security, they could mean the difference between saving incalculable sums of money and assets.

Multi-Criteria Decision-Making has the potential to improve all aspects of engineering decision-making, from design to manufacturing. However, it is especially useful for applications in high-tech market sectors, where product differentiation and competitive advantage are frequently achieved by merely making very small improvements in material performance. According to Tao et al. (2020), the capacity of MCDM techniques to simultaneously take into account material, process, and shape for challenging material selection issues exemplifies their full potential. Therefore, it is crucial to extend the use of MCDM techniques to a wide range of engineering applications and to learn from past experiences in order to enhance material selection. Practical design issues include the need to deal with uncertainty and compromise, and the effective manipulation of data ranges is essential to a more efficient use of MCDM in material selection and design (Wu, 2022). A significant area in which MCDM is beginning to benefit is the selection of more advanced materials and materials with specialized properties, particularly composites and multi-functional materials. Multi-criteria analysis capability is desirable for future versions of computer simulation software due to the current emphasis on materials design and modeling.

7 Conclusion:

Companies and developers must take a more proactive approach to security concerns during the mobile app development process. Researchers have compiled several areas that the developers can address when building apps, even though there are many things to look for in terms of security. As part of the software development process, application developers conduct application security testing to ensure that new or updated software applications do not contain security flaws. This exercise demands the presentation of informed decisions that can help in the implementation of the conducts. An attacker can get around the app security during authentication and authorization decisions based on the input values.

A focus on the various MCDM models for allowing the security technicians to deal with the security concerns in development of team has been discussed. The model's interaction has been assessed and the aspects of sensitivity and the Techniques for enhancing an

application's security at the coding level and making it less susceptible addressed in efforts to see the threats are known based on application security controls.

8 References

Bączkiewicz, A., Kaczyńska, A., & Wątróbski, J. (2021). Study on objectivity of mobile phone preferences: the MCDA analysis. *Procedia Computer Science*, *192*, 5067–5080. https://doi.org/10.1016/j.procs.2021.09.285

Bhole, G. P. (2018). Multi Criteria Decision Making (MCDM) Methods and its applications. *International Journal for Research in Applied Science and Engineering Technology*, *6*(5), 899–915. https://doi.org/10.22214/ijraset.2018.5145

Waxler, J., 2018. *Prioritizing Security Controls Using Multiple Criteria Decision Making for Home Users* (Doctoral dissertation, The George Washington University).

Borissova, D. (2021) 'An overview of multi-criteria decision-making models and software systems', in *Studies in Computational Intelligence*. Cham: Springer International Publishing, pp. 305–323.

Chen, E. Y. *et al.* (2014) 'OAuth Demystified for Mobile Application Developers', in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: ACM.

Costa, P. *et al.* (2019) 'The security challenges emerging from the technological developments: A practical case study of organizational awareness to the security

risks', *Mobile networks and applications*, 24(6), pp. 2032–2037. doi: 10.1007/s11036-018-01208-0.

Daradkeh, M. K. and Sabbahein, H. A. S. (2019) 'Factors influencing the adoption of mobile application development platforms: A qualitative content analysis of developers' online reviews', *International journal of enterprise information systems*, 15(4), pp. 43–59. doi: 10.4018/ijeis.2019100103.

Ettiane, R., Chaoub, A. and Elkouch, R. (2021) 'Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions', *Journal of information security and applications*, 61(102943), p. 102943. doi: 10.1016/j.jisa.2021.102943.

Gardner, J. *et al.* (2022) 'Helping mobile application developers create accurate privacy labels', in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE.

Han, Y. *et al.* (2016) 'A feature-oriented mobile software development framework to resolve the device fragmentation phenomenon for application developers in the mobile software ecosystem', in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Cham: Springer International Publishing, pp. 189–199.

Jahkola, O. *et al.* (2017) 'What should application developers understand about mobile phone position data', in *Proceedings of the 18th International Conference on Computer Systems and Technologies*. New York, NY, USA: ACM.

Kabassi, K. (2022) 'Comparison of multi-criteria decision-making models: Analyzing the steps in the domain of websites' evaluation', *International journal of information technology & decision making*, 21(02), pp. 729–753. doi: 10.1142/s0219622021500590.

Karande, A. M. and Joshi, P. (2022) 'Multi-criteria decision making for software vulnerabilities analysis', in *Multi-Criteria Decision Models in Software Reliability*. Boca Raton: CRC Press, pp. 201–217.

Khan, S. A., Khan, W., & Pandey, D. (2021). A fuzzy multi-criteria decision-making method for managing network security risk perspective. In *Cloud-Based Big Data Analytics in Vehicular Ad-Hoc Networks* (pp. 115–140). IGI Global.

Ksibi, S., Jaidi, F. and Bouhoula, A. (2022) 'A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach', *Mobile networks and applications*. doi: 10.1007/s11036-022-02042-1.

M. Venkata Krishna Reddy, P.V.S. Srinivas and M. Chandra Mohan (2022) 'Enhancing the routing security through node trustworthiness using secure trust based approach in mobile Ad Hoc Networks', *International Journal of Interactive Mobile Technologies (iJIM)*, 16(14), pp. 152–170. doi: 10.3991/ijim.v16i14.30651.

Maliene, V., Dixon-Gough, R., & Malys, N. (2018). Dispersion of relative importance values contributes to the ranking uncertainty: Sensitivity analysis of Multiple Criteria Decision-Making methods. *Applied Soft Computing*, *67*, 286–298. https://doi.org/10.1016/j.asoc.2018.03.003

Michael Ogata, Josh Franklin, Jeffrey Voas, Vincent Sritapan, Stephen Quirolgico (2019) *Vetting the Security of Mobile Applications*. NIST Special Publication 800-163 Revision 1: https://doi.org/10.6028/NIST.SP.800-163r1.

Poovendran, R. and Saad, W., 2014. Decision and Game Theory for Security. Lecture Notes in Computer Science, 8840.

Russello, G., Lioy, A., Prasad, N.R. and Lian, S., 2010. Security and Privacy in Mobile Information and Communication Systems. Springer Berlin Heidelberg.

Samantraj, S., Dash, S., & Patnaik, P. K. (2020). Mobile device transmission security policy decision making using PROMETHEE. In *Machine Learning and Information Processing* (pp. 1–9). Springer Singapore.

Sarker, I. H. *et al.* (2022) 'Internet of things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions', *Mobile networks and applications*. doi: 10.1007/s11036-022-01937-3.

Saunders, M., (2012). *Research Methods for Business Students.* 6th Edition ed. s.l.:Pearson Education.

Song, J. *et al.* (2018) 'Platform adoption by mobile application developers: A multimethodological approach', *Decision support systems*, 107, pp. 26–39. doi: 10.1016/j.dss.2017.12.013.

Strzelecki, A. (2020) 'Application of developers' and users' dependent factors in App Store optimization', *International Journal of Interactive Mobile Technologies (iJIM)*, 14(13), p. 91. doi: 10.3991/ijim.v14i13.14143.

Suomalainen, J. *et al.* (2022) 'Security-driven prioritization for tactical mobile networks', *Journal of information security and applications*, 67(103198), p. 103198. doi: 10.1016/j.jisa.2022.103198.

Tan, T., Mills, G., Papadonikolaki, E., & Liu, Z. (2021). Combining multi-criteria decision making (MCDM) methods with building information modelling (BIM): A review. *Automation in Construction*, *121*(103451), 103451. https://doi.org/10.1016/j.autcon.2020.103451

Tao, C., Guo, H. and Huang, Z. (2020) 'Identifying security issues for mobile applications based on user review summarization', *Information and software technology*, 122(106290), p. 106290. doi: 10.1016/j.infsof.2020.106290.

Teymourzadeh, M., Dept. of Computer Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran and Javdani Gandomani, T. (2017) 'Introducing a particular quality model in mobile application development: The mobile application developers' perspective', *Journal of software*, 12(5), pp. 339–347. doi: 10.17706/jsw.12.5.339-347.

Wu, X. (2022) ‘Special issue on advanced network security: Methods and applications’, *Mobile networks and applications*, 27(4), pp. 1337–1338. doi: 10.1007/s11036-022-01983-x.

Yasumatsu, T. *et al.* (2019) ‘Understanding the responsiveness of mobile app developers to software library updates’, in *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*. New York, NY, USA: ACM.

Zaidi, A. Z. *et al.* (2022) ‘A framework of dynamic selection method for user classification in touch-based continuous mobile device authentication’, *Journal of information security and applications*, 67(103217), p. 103217. doi: 10.1016/j.jisa.2022.103217.