Texas A&M University - Commerce

Department of Computer Science

The Detailed Analysis of Cyber Attacks and Their Countermeasures to Prevent Them Effectively

Mounika Malka

Supervisor: Derek Harter, Ph.D.

A report submitted in partial fulfilment of the requirements of
Texas A&M University - Commerce for the degree of
Master of Science in *Computer Science*

February 5, 2024

Declaration

I, Mounika Malka, of the Department of Computer Science, Texas A&M University - Commerce, confirm that this is my own work and figures, tables, equations, code snippets, artworks, and illustrations in this report are original and have not been taken from any other person's work, except where the works of others have been explicitly acknowledged, quoted, and referenced. I understand that if failing to do so will be considered a case of plagiarism. Plagiarism is a form of academic misconduct and will be penalised accordingly.

I give consent to a copy of my report being shared with future students as an exemplar.

I give consent for my work to be made available more widely to members of TAMUC and public with interest in teaching, learning and research.

Mounika Malka
February 5, 2024

Abstract

Cybersecurity, nowadays, is a spiral apprehension in the technological ecosystem. This exploration investigates the powerful scene of cyberattacks, accentuating advancing patterns, preventive techniques, and moderation measures. Grounded in a blended techniques approach, it coordinates quantitative information on purchaser mindfulness with subjective experiences from contextual investigations and master interviews. The review expects to give nuanced understanding and viable bits of knowledge for associations to reinforce their advanced guards. Enhancing the resilience of digital systems, influencing strategies, and improved cybersecurity discourse are among the anticipated outcomes. A coherent investigation of the dynamics of cybersecurity is made easier by the structured report's navigation through the introduction, background, methodology, discussion, and conclusions.

Acknowledgements

An acknowledgements section is optional. You may like to acknowledge the support and help of your supervisor(s), friends, or any other person(s), department(s), institute(s), etc. If you have been provided specific facility from department/school acknowledged so.

Contents

List of Figures

List of Tables

List of Abbreviations

SMPCS	School of Mathematical, Physical and Computational Sciences

Chapter 1

Introduction

1.1 Introduction

The prospect of frequent cyberattacks has flattered a persistent and widening affair in the present's constantly switching digital domain. Securing digital estates bestows conspicuous drawbacks, as comprehended by the current expansion in the figure and smoothness of this onslaught. Subsequently, malignant actors' tactics progress accompanying apparatus; it is imperious to take obstructive considerations to condense susceptibilities. To evade and diminish these constant switching hazards, this thesis commenced an intensive study, imparting the convolutions of cyberattacks and bestowing pragmatic fortifications

1.2 Background of the study

Background of the study This paper's entourage depicts the authentic expansion of cyberattacks, a diffuse interpretation of how they flourished from the prior dawning to the cosmopolitan hazards of today. Eloquent locus these hazards hit from and where they switch extinct time is determining in the constantly expanding province of cybersecurity. In diffuse of the augment integer of cyberattacks, the hitch of alternative becomes prominent, accentuating the prerequisite of felicitous fortification. This thesis disposes itself enclosed by the body of the bibliography on cybersecurity, conceding the inventive chores of Strbac Savić and Tomašević (2012) in the province and appending to the present discussion on cybersecurity by intercepting the straining of averting and appeasing cyberattacks.

1.3 Research Question

Research Question

- What are the evolving patterns and tactics of cyber-attacks, and how can organizations develop comprehensive and adaptive countermeasures to effectively prevent and mitigate these attacks in an ever-changing cybersecurity landscape.
- What are the current trends and methods used in cyber-attack and how they have evolved in time?

- How can the organisation development be to prevent the cyber-attack that consider dynamic nature of the cyber security landscape?
- What's specific counter measure can organised implement for mitigating the impact of evolving cyber threat?
- What role do adaptability and continuous improvement play in the face of rapid changing cyber threat in the development of successful cyber security defence for organisation?

1.4 Research Hypothesis

Research Hypothesis

- H1: Cyberattack victory outlay harmonizes with greater consumer consciousness..
- H0: The ascending mechanism of cyberattack susceptibilities needs to be revised.

1.5 Scope and Context of the Project

Scope and Context of the Project The scope of the project is used to encompass a comprehensive examination of the cyber threat and define strategies that emphasize digital systems. It focused on the evolving landscape of cyberattack attacks that also investigated consumers' awareness of the impact of cyber fortification. This research also contributes to the practical inside of safeguarding in the digital domain. The context of the study indicates the realm of cybersecurity. It addresses the major of the agency that evolves practices of malicious actors by providing an understanding of the cyber security practices.

1.6 Aims and Objectives of the Project

Aims and Objectives of the Project Aims The project aims to understand contemporary cyber issues and vulnerabilities in the digital system and the role of consumer awareness, which also cultivates the practical inside for robust cyber fortification strategies

1.7 Objective

Objective

- To finds the current trends and methods used in cyber-attack and how they have evolved in time
- To identify the organisation development to prevent the cyber-attack that consider dynamic nature of the cyber security landscape
- To find out the specific counter measure can organised implement for mitigating the impact of evolving cyber threat

- To identify the role, do adaptability and continuous improvement play in the face of rapid changing cyber threat in the development of successful cyber security defence for organisation.

1.8 Methodological Approach

Methodological Approach The current study employs a mixed methods approach that incorporates both quantitative and qualitative methods. The comprehensive study forms the foundation analyzing the existing theories as well as empirical studies on the cyber threat and fortification. Quantitative data will be gathered through the help of services that help assess consumer awareness and preferences. On the other hand, the qualitative data will improve health through the case studies as well as expert interviews that also offer in-depth analysis in effective cyber threat strategies. This synthesis of the methods provides an understanding of the cyber threat in a holistic way that also fortifies the tactics and the interpreter between consumer awareness with the cyber security measures.

Chapter 2

Literature Review

2.1 Introduction

The possibility of continuous cyberattacks has complemented a tenacious and broadening issue in the current steady exchange of computerized space. Getting computerized homes gives prominent disadvantages, as fathomed by the ongoing extension in the figure and perfection of these attacks. Accordingly, harmful entertainers' strategies progress going with the contraption, it is imperious to take obstructive contemplation to consolidate susceptibilities. By avoiding and lessening these steady exchanging dangers, this proposition started an escalated study, giving the convolutions of cyberattacks. The essential focal point of the section is to feature and assess the most dependable study in light of the examination subject of the adequacy of the latest things and techniques utilized in digital assault and the association's advancement to forestall the digital assault that considers the dynamic nature of cyber-security. This section has involved ideas regarding characterizing the meaning of the examination subject. In this way, the literature has fostered its key idea in light of applicable studies given the referenced exploration subject as far

2.2 Discussion on the Current Trends and Methods used in Cyber-Attack

The dynamic landscape of cyber security has created a battleground for hackers and security providers. With the advancement of technology, the methods are upgraded by malicious hackers to exploit the vulnerability. The current trends and methods in the cyber attack will be determined below:

- Remote working cyber security risk

  The remote work generated by the COVID-19 pandemic opened up new cyber issues for organizations as well as individuals. Remote officers are often less fortified than the centralized office, which becomes a breeding ground for cyber hackers (Kaspersky, 2019). The use of personal devices that link professional life and personal life impacts the risk of sensitive information falling into the wrong hands. Organizations need to develop and identify security vulnerabilities by improving their system of implementing control that ensures proper monitoring for a secure distributed workforce.

- IoT evolution The Internet of Things (IoT) is growing, providing cybercriminals with a larger attack surface. IoT devices, fluctuating from wearables to keen home strategies, repeatedly lack rigorous security actions (Kaspersky, 2019). This absence generates challenges in retaining outdated security claims, making IoT a well-paid target. As the quantity of IoT strategies is predicted to reach 64 billion worldwide by 2026, administrations must augment their safety posture to precaution in contradiction of latent occurrences.

- The rise of Ransomware A persistent threat, Ransomware, has been a surge in sophistication with frequency. The improving digitization landscape during the time of pandemic has upgraded the remote work that provided cyber criminals with their target (Kaur and Kumar K.R, 2021). The attacks involve encryption of companies' data that provides a threat for releasing sensitive information. The financial and reputation consequences of the attacks have been identified as creating a concern for the companies.

- Cloud services with security threats the boundless reception of cloud administrations has reformed how organizations work; however, it has likewise become an ideal objective for digital aggressors (Kaur and Kumar K.R, 2021). Misconfigured cloud settings, uncertain Points of interaction, and record seizing present serious dangers. According to Cabaj et al. (2018), associations should address difficulties connected with administrative consistency, IT aptitude, and potential section focuses on assailants, building up their cloud safety efforts.

- Smarter social engineering attack ' The engineering attacks have become more sophisticated for cyber hackers, as they target remote workers. The most innovative social attacks focused on the leadership of the organization, smashing and vising. Cyber hackers constantly improve their platforms in innovative ways, like messaging apps, to trick users.

- Data privacy The high-profile data breaches with the data protection law have elevated the organization's privacy.However,noncompliance risks reputational damage and loss of trust can impact the organization created by cyber hackers. As per the view of Cabaj et al. (2018), organizations are focused on data privacy by appointing data privacy officers, implementing encryption, and undergoing external assessment.

- Multi-factor authentication improvement While MFA is viewed as a strong verification strategy, aggressors track down ways of bypassing it, primarily through SMS or telephone-based confirmation. Associations are moving towards application-based MFA to address weaknesses related to SMS validation. To stay ahead of malicious actors, MFA methods must continue to evolve.

- Rise of AI tools The cyber threat has led organizations to leverage AI and machine learning for analyzing security infrastructure. AI aids in the automatic security system for threat detection and data analysis for human capability at a pace beyond the capability of humans.As per the statement of Cabaj et al. (2018), the automatic attacks for AI tools have been developed by data-driven security tools of cyber hackers.

- Mobile cyber security With the high usage of remote working mobile devices have become more Central for everyday operation. The ever-trending usage of mobile has improved the mobile threads that include spyware security vulnerabilities with the malware software of mobile. As the 5G technology rollout, organisations are impacted by more cyber hackers.

The cyber threats in the dynamic technology progress have been updated due to the 5G network progress.

2.3 Identification of the Organization's Development to Prevent the Cyber-Attack

Protecting against cyber-attacks requires incorporating policies and education technology with ongoing development. The organizations that face issues with cyber security need to develop these measures in the dynamic nature of the cyber threat:

- Continuous network and database security Safeguard the organizations by setting up firewalls and scrambling data. This will assist with limiting the gamble of digital hoodlums accessing secret data. Ensure the Wi-Fi network is covered up and the secret phrase is safeguarded. Be careful when selecting the data that is saved in the company databases. As stated by Mass (2023), data sets can be an incredible means for organizations to have a focal area of information and reports, yet this doesn't mean putting away all information is positive. Programmed upholding of organization information ought to be set to be finished either one time each day or one time each week, contingent upon the degree of action inside the organization. Backing up the organization's information will improve the probability of a digital assault. Hence, the organization's information won't be lost totally, which is very much standard.

- Employee education with training Educating the employees is an aspect of strengthening the cyber security posture for the company. On the other hand, the conduction of training programs can also raise awareness of the importance of cyber security in the organization. As opined by Mass (2023), transparent communication systems with employees provide safeguards for the company that also provides security for customer data and colleagues' details. Establishing enforcement policies delineating acceptable practices also leaves it the axis for minimizing the risk of downloading malicious software.

- A security policy with practices The comprehensive security policies in the organization are tailored to the practice with specific needs. These guidelines cover several aspects, including data protection, data security, and network security with incident response. By clearly outlining the procedure for the following in the event of a security bridge, the policy violation also decreases (Mohamed, 2023). However, controlling physical access to the company ensures the proper disposable procedure. It also has to prevent authorized access to the computer system or handling devices that reduce the likelihood of cyber threats.

- Awareness of fake antivirus offers Employee training helps to recognize and distinguish them from fake antivirus offers and notifications. However, by developing a clear policy for reporting suspicious activity the cyber hackers often used the tactic to track the users for downloading malicious software (Mohamed, 2023). Establishing a protocol for handling the infected computers emphasizes the importance of reporting to the IT department. Additionally, regular updates to the security software provide safeguards against the cyber security threat.

- Customer communication protection Building trust and ensuring the security of customers' personal information require open lines of communication—expressive explanations behind gathering client information and how it will be utilized. The narrator of Cs et al. (2017) guarantees clients that the association won't ever demand touchy data through unprotected correspondence channels, such as email or instant messages. Urge clients to report dubious correspondences, cultivating a cooperative way to deal with online protection.

- Dynamic organization development Companies must impress the adaptive approaches of cyber security to prevent cyber attacks. It includes ongoing assistance in enhancing the security measures in responding to emerging threats. However, implementing regular risk assessment with the scan of vulnerability can find the potential weaknesses in the security infrastructure. For instance, key-logging malware can follow all that the client types on their console. This implies digital lawbreakers could access financial balances, client data, passwords, and other organisation delicate data. As narrated by Cs et al. (2017), to stay up with the latest to help forestall malware from sneaking into your framework and organizations. On the other hand, a faster culture for continuous improvement also provides cyber security practices that update with the evolving threat of the landscape.

- Collaboration and information sharing Collaboration with industrial information sharing is an essential component of cyber security. By engaging with the cyber security communities, the organization can identify threat intelligence by sharing initiatives and findings about the latest trends with attack vectors (Rajasekharaiah et al., 2020). On the other hand, collaboration with other fields of organization and business can gain valuable insight into emerging ideas for threats that contribute to a cyber security strategy in a resilient way.

Table 2.1: SWOT Analysis for Cybersecurity Countermeasures

Strength	Weakness
Firewall protection	Lack of mobile security
Regular data backups with security	insufficient employee awareness
Updated anti-virus software	Third party authentication
Training programs of employees	Limited response plan

Table 2.2: SWOT Analysis for Cybersecurity Countermeasures

Opportunities	Threats
Advances in cloud computing	Evolving Phishing techniques
Emerging in authentication tech	Increase Iot Vulnerabilities
Integration with AI security	Ransomware attacks
Collaboration with cyber security community	Regulatory landscape of cyber security

Analysis

Strength A strong firewall has provided a foundation and defense for authorized access. A regular update in optimizing the protection is crucial for preventing a cyber attack. On the other

hand, consistent data backup also reduces the impact of ransom attacks and minimizes the nation of the downtown in the event of a breach (Cremer et al., 2022). By keeping up the antivirus software, it has enhanced the ability to detect malware, which reduces the risk of infections. Investing in continuous employee training programs provides identification of potential security threats.

Weakness The efficient awareness among the employees increases the vulnerability through which the training programs of education are essential for empowering the workforce to address cyber security threats (Cremer et al., 2022). However, a comprehensive incident response plan is crucial for mitigating the impact of cyber attacks. A regular testing plan to enhance cyber security is necessary for Swift and effective response (Radanliev et al., 2020). Falling to ensure the security of third-party vendors can also impact the organization to its security structure. With the high rise of remote work and mobile security is implementing a robust measure for securing company data.

Opportunities Artificial intelligence for threat detection is responsible for helping to enhance the ability of organisations to evolve cyber threats (Radanliev et al., 2020). Engaging in the threat intelligence sharing initiative provides organizations with them to stay focused on emerging threads that help to adopt proactive countermeasures. Implementation of technological developments in cloud security confirms a vigorous and ascendable defense against developing cyber pressures (Altulaihan et al., 2022). Adopting new confirmation means, such as biometrics or multi-factor confirmation, fortifies access joysticks.

Threats Threats Cybercriminals unceasingly refine phishing methods. Often, bringing up-to-date and underpinning operative training curricula is critical to hostage evolving pressures (Altulaihan et al., 2022). The cumulative cleverness of ransomware poses a noteworthy threat. Regular reviewing and apprising occurrence response strategies are indispensable for modifying the impression of ransomware occurrences. The growing Internet of Things surges the attack shallow (Riggs et al., 2023). The Establishment of IoT security actions is serious about preventing possible breaches. Acquiescence with managerial requirements is motivating but crucial. Solid audits and up-to-date refuge policies are required to pilot a complex monitoring countryside.

2.4 Identification of the role that plays in the face of rapidly changing cyber threat in cyber security defense for organization

The Role of cybersecurity Defence for organizations is securing the organization's data from internal and External threats. This involves a wide range of technologies, processes, structures, and practices aimed at safeguarding networks, computers, programs, and data against unauthorized access or damage (B. Poornima, 2023). At its core the cybersecurity team is tasked with shielding the IT infrastructure from vulnerabilities, implementing security measures, monitoring suspicious activities, and swiftly responding to the cyber threat. Their collaborative efforts with the other departments aim to enhance the organization's overall security posture. The Security Operations Center (SOC) plays a pivotal role in organizational security, with distinct team responsibilities. Security Analysts conduct real-time vulnerability assessments and monitor threat intelligence. Incident Responders excel in immediate response and disaster recovery during security breaches. Security Architects strategically plan, design, and review the overall security posture (Cynet, 2023). This collaborative approach ensures a comprehensive defense against cyber threats, addressing both immediate incidents and fortifying the organization's long-term security resilience.

Cybersecurity professionals, as strategists, proactively implement security measures, considering consequences and evaluating workflows, dependencies, and resources. They stay ahead of evolving hacking methods by studying entry points and countermeasures (Cynet, 2023). As communicators, management and interpersonal skills are crucial for effective coordination. Being lifelong learners, they maintain technical competence through continuous research, training, and certifications, addressing complex security challenges.

The Important Roles of Cybersecurity :

- Leadership Responsibilities of the CISO: the CISO plays a crucial leadership role in the cybersecurity department and provides direction on various programs, including audits and risk management (Book, 2023).
- One essential focus is security analysis, involving the gathering of threat intelligence and monitoring the potential vulnerabilities in security systems.
- The security engineers construct and maintain the security architecture, ensuring up-to-date endpoint protection and software development (Book, 2023).
- The incident response plays a vital role during a cyber attack by leading the development and execution of incidence response strategies to minimize the damages.

  Cybersecurity departments employ various defensive measures to protect against cyber threats. Establishing a robust Cybersecurity Awareness Training Program is crucial for organizational resilience. The program should emphasize the significance of a data backup strategy within the broader security framework, stressing its role in disaster recovery and business continuity. Addressing Common Vulnerabilities and Exposures (CVEs) is essential, providing insights into system-specific security risks (Book, 2023). Introducing Extended Detection and Response (XDR) solutions is recommended, offering a proactive approach to detect and respond to unauthorised access and cyber threats comprehensively. Cynet's innovative monitoring of endpoint memory, focusing on identifying exploit-like behavior, further enhances the organization's defense against evolving cyber risks.

2.5 Theoretical Underpinning

Fortifying Cyber Security: Embracing Theoretical Framework Against Cyber Attack Welsh Security Theory The Welsh Security Theory, often referred to as the "Security Onion" model, plays a crucial role in mitigating cyber security threats within organizations. This model advocates for a layered and comprehensive approach to security, establishing a robust defense-in-depth strategy (Ifac, 2023). By incorporating various defense measures such as firewalls, antivirus software, intrusion detection systems, and user training, the Security Onion model creates a multi-faceted security framework. The interconnected layers work together to fortify the organization's defenses, making it more challenging for cyber threats to breach. Furthermore, the model emphasizes continuous monitoring, incident response planning, and collaborative efforts, fostering adaptability and resilience in the face of evolving cyber threats. Implementation of the Welsh Security Theory enhances overall security resilience, reducing vulnerabilities in the dynamic landscape of cyber threats.

Copenhagen Security Theory

The Copenhagen School's securitization theory was initially formulated for traditional security issues and can be adapted to enhance cyber security defense. In the context of cybersecurity, securitization involves framing specific cyber threats as existential risks, gaining acknowledgment from the audience, and allowing for extraordinary measures. By applying securitization theory, organizations can prioritize cyber threats effectively, elevating them above routine concerns (Diskaya, 2013). This facilitates allocating resources, attention, and swift responses to potential cyber risks. The identification of cyber threats as existential can lead to the implementation of robust defense mechanisms and the development of emergency response plans. Furthermore, the Copenhagen School's emphasis on desecuritization can be valuable. Shifting issues back into the ordinary public sphere means addressing cyber threats within the context of routine practices rather than treating them as exceptional. This approach encourages a continuous, integrated, and normalized cybersecurity strategy, fostering resilience against evolving cyber threats.

2.6 Literature gap

The general writing audit part can be characterized to be viable as far as framing the viability of network protection for associations or people in diminishing Digital Assault. In any case, a few huge holes can be characterized in this part connected with the social event of data. The writing papers considered in this section have not had the option to give explicit models concerning the examination subject. Besides, it very well may be featured that the section could incorporate more applicable examination papers in light of the subject. Consequently, these holes in the writing part can be featured which could be dispensed with.

2.7 Summary

The literature review offers an inclusive overview of the active scenery of cyber sanctuary, the importance of the current drifts, and approaches employed by cyber aggressors. The escalating risks related to isolated working, IoT fruition, ransomware, cloud amenities, communal commerce, data discretion, multi-factor confirmation, AI, and mobile cybersecurity require administrations to adopt practical and adaptive approaches. The operation of the Welsh Security Theory and Copenhagen Security Theory appears as appreciated frameworks, stressing defense-in-depth and secularization ideologies. The recognized countermeasures, shown through SWOT analysis, recommend a deliberate road map for administrations to increase their cybersecurity carriage. The embryonic role of cybersecurity in the aspect of quickly changing pressures emphasizes the position of control tasks, security analysis, occasion response, and collective efforts. Regardless of the overall success of the literature, there is a gap in as long as specific specimens and more germane research credentials on the preferred exploration topic, portentous avenues for forthcoming investigation.

Chapter 3

Methodology

We mentioned in Chapter 1 that a project report's structure could follow a particular paradigm. Hence, the organization of a report (effectively the Table of Content of a report) can vary depending on the type of project you are doing. Check which of the given examples suit your project. Alternatively, follow your supervisor's advice.

3.1 Examples of the sections of a methodology chapter

A general report structure is summarised (suggested) in Table 3.1. Table 3.1 describes that, in general, a typical report structure has three main parts: (1) front matter, (2) main text, and (3) end matter. The structure of the front matter and end matter will remain the same for all the undergraduate final year project report. However, the main text varies as per the project's needs.

3.1.1 Example of a software/Web development main text structure

Notice that the "methodology" Chapter of Software/Web development in Table 3.2 takes a standard software engineering paradigm (approach). Alternatively, these suggested sections can be the chapters of their own. Also, notice that "Chapter 5" in Table 3.2 is "Testing and Validation" which is different from the general report template mentioned in Table 3.1. Check with your supervisor if in doubt.

3.1.2 Example of an algorithm analysis main text structure

Some project might involve the implementation of a state-of-the-art algorithm and its performance analysis and comparison with other algorithms. In that case, the suggestion in Table 3.3 may suit you the best.

3.1.3 Example of an application type main text structure

If you are applying some algorithms/tools/technologies on some problems/datasets/etc., you may use the methodology section prescribed in Table 3.4.

Table 3.1: Undergraduate report template structure

Frontmatter		Title Page Abstract Acknowledgements Table of Contents List of Figures List of Tables List of Abbreviations
Main text	Chapter 1	Introduction
	Chapter 2	Literature Review
	Chapter 3	Methodology
	Chapter 4	Results
	Chapter 5	Discussion and Analysis
	Chapter 6	Conclusions and Future Work
	Chapter 7	Refection
End matter		References Appendices (Optional) Index (Optional)

Table 3.2: Example of a software engineering-type report structure

Chapter 1	Introduction	
Chapter 2	Literature Review	
Chapter 3	Methodology	
		Requirements specifications
		Analysis
		Design
		Implementations
Chapter 4	Testing and Validation	
Chapter 5	Results and Discussion	
Chapter 6	Conclusions and Future Work	
Chapter 7	Reflection	

3.1.4 Example of a science lab-type main text structure

If you are doing a science lab experiment type of project, you may use the methodology section suggested in Table 3.5. In this kind of project, you may refer to the "Methodology" section as "Materials and Methods."

Table 3.3: Example of an algorithm analysis type report structure

Chapter 1	Introduction	
Chapter 2	Literature Review	
Chapter 3	Methodology	
		Algorithms descriptions
		Implementations
		Experiments design
Chapter 4	Results	
Chapter 5	Discussion and Analysis	
Chapter 6	Conclusion and Future Work	
Chapter 7	Reflection	

Table 3.4: Example of an application type report structure

Chapter 1	Introduction	
Chapter 2	Literature Review	
Chapter 3	Methodology	
		Problems (tasks) descriptions
		Algorithms/tools/technologies/etc. descriptions
		Implementations
		Experiments design and setup
Chapter 4	Results	
Chapter 5	Discussion and Analysis	
Chapter 6	Conclusion and Future Work	
Chapter 7	Reflection	

Table 3.5: Example of a science lab experiment-type report structure

Chapter 1	Introduction	
Chapter 2	Literature Review	
Chapter 3	Materials and Methods	
		Problems (tasks) description
		Materials
		Procedures
		Implementations
		Experiment set-up
Chapter 4	Results	
Chapter 5	Discussion and Analysis	
Chapter 6	Conclusion and Future Work	
Chapter 7	Reflection	

3.2 Example of an Equation in LaTeX

Eq. 3.1 [note that this is an example of an equation's in-text citation] is an example of an equation in LaTeX. In Eq. (3.1), s is the mean of elements $x_i \in \mathbf{x}$:

$$s = \frac{1}{N} \sum_{i=1}^{N} x_i. \tag{3.1}$$

Have you noticed that all the variables of the equation are defined using the **in-text** maths command $.$, and Eq. (3.1) is treated as a part of the sentence with proper punctuation? Always treat an equation or expression as a part of the sentence.

3.3 Example of a Figure in LaTeX

Figure 3.1 is an example of a figure in LaTeX. For more details, check the link:
wikibooks.org/wiki/LaTeX/Floats,_Figures_and_Captions.
Keep your artwork (graphics, figures, illustrations) clean and readable. At least 300dpi is a good resolution of a PNG format artwork. However, an SVG format artwork saved as a PDF will produce the best quality graphics. There are numerous tools out there that can produce vector graphics and let you save that as an SVG file and/or as a PDF file. One example of such a tool is the "Flow algorithm software". Here is the link for that: flowgorithm.org.

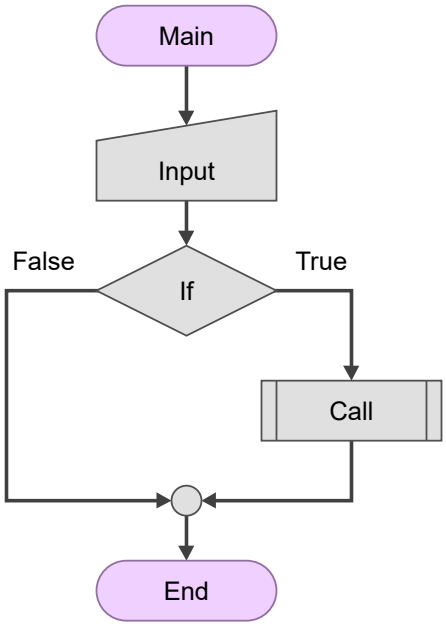

Figure 3.1: Example figure in LaTeX.

3.4 Example of an algorithm in LaTeX

Algorithm 1 is a good example of an algorithm in LaTeX.

Algorithm 1 Example caption: sum of all even numbers

Input: $\mathbf{x} = x_1, x_2, \ldots, x_N$
Output: $EvenSum$ (Sum of even numbers in $\mathbf{x}$)

1: **function** EvenSummation($\mathbf{x}$)
2: $EvenSum \leftarrow 0$
3: $N \leftarrow length(\mathbf{x})$
4: **for** $i \leftarrow 1$ to N **do**
5: **if** $x_i \mod 2 == 0$ **then** ▷ check if a number is even?
6: $EvenSum \leftarrow EvenSum + x_i$
7: **end if**
8: **end for**
9: **return** $EvenSum$
10: **end function**

3.5 Example of code snippet in LaTeX

Code Listing 3.1 is a good example of including a code snippet in a report. While using code snippets, take care of the following:

- do not paste your entire code (implementation) or everything you have coded. Add code snippets only.
- The algorithm shown in Algorithm 1 is usually preferred over code snippets in a technical/-scientific report.
- Make sure the entire code snippet or algorithm stays on a single page and does not overflow to another page(s).

Here are three examples of code snippets for three different languages (Python, Java, and CPP) illustrated in Listings 3.1, 3.2, and 3.3 respectively.

```python
import numpy as np

x  = [0, 1, 2, 3, 4, 5] # assign values to an array
evenSum = evenSummation(x) # call a function

def evenSummation(x):
    evenSum = 0
    n = len(x)
    for i in range(n):
        if np.mod(x[i],2) == 0: # check if a number is even?
            evenSum = evenSum + x[i]
    return evenSum
```

Listing 3.1: Code snippet in LaTeX and this is a Python code example

Here we used the "\clearpage" command and forced-out the second listing example onto the next page.

```java
public class EvenSum{
    public static int evenSummation(int[] x){
        int evenSum = 0;
        int n = x.length;
        for(int i = 0; i < n; i++){
            if(x[i]%2 == 0){ // check if a number is even?
                evenSum = evenSum + x[i];
            }
        }
        return evenSum;
    }
    public static void main(String[] args){
        int[] x  = {0, 1, 2, 3, 4, 5}; // assign values to an array
        int evenSum = evenSummation(x);
        System.out.println(evenSum);
    }
}
```

Listing 3.2: Code snippet in LaTeX and this is a Java code example

```cpp
int evenSummation(int x[]){
    int evenSum = 0;
    int n = sizeof(x);
    for(int i = 0; i < n; i++){
        if(x[i]%2 == 0){ // check if a number is even?
            evenSum = evenSum + x[i];
      }
    }
    return evenSum;
}

int main(){
    int x[]  = {0, 1, 2, 3, 4, 5}; // assign values to an array
    int evenSum = evenSummation(x);
    cout<<evenSum;
    return 0;
}
```

Listing 3.3: Code snippet in LaTeX and this is a C/C++ code example

3.6 Example of in-text citation style

3.6.1 Example of the equations and illustrations placement and reference in the text

Make sure whenever you refer to the equations, tables, figures, algorithms, and listings for the first time, they also appear (placed) somewhere on the same page or in the following page(s). Always make sure to refer to the equations, tables and figures used in the report. Do not leave them without an **in-text citation**. You can refer to equations, tables and figures more them once.

3.6.2 Example of the equations and illustrations style

Write **Eq.** with an uppercase "Eq" for an equation before using an equation number with (\eqref{.}). Use "Table" to refer to a table, "Figure" to refer to a figure, "Algorithm" to

refer to an algorithm and "Listing" to refer to listings (code snippets). Note that, we do not use the articles "a," "an," and "the" before the words Eq., Figure, Table, and Listing, but you may use an article for referring the words figure, table, etc. in general.

For example, the sentence "A report structure is shown in **the** Table 3.1" should be written as "A report structure is shown **in** Table 3.1."

3.7 Summary

Write a summary of this chapter.

Note: In the case of **software engineering** project a Chapter "**Testing and Validation**" should precede the "Results" chapter. See Section 3.1.1 for report organization of such project.

Chapter 4

Results

The results chapter tells a reader about your findings based on the methodology you have used to solve the investigated problem. For example:

- If your project aims to develop a software/web application, the results may be the developed software/system/performance of the system, etc., obtained using a relevant methodological approach in software engineering.
- If your project aims to implement an algorithm for its analysis, the results may be the performance of the algorithm obtained using a relevant experiment design.
- If your project aims to solve some problems/research questions over a collected dataset, the results may be the findings obtained using the applied tools/algorithms/etc.

Arrange your results and findings in a logical sequence.

4.1 A section

...

4.2 Example of a Table in LaTeX

Table 4.1 is an example of a table created using the package LaTeX"booktabs." do check the link: wikibooks.org/wiki/LaTeX/Tables for more details. A table should be clean and readable. Unnecessary horizontal lines and vertical lines in tables make them unreadable and messy. The example in Table 4.1 uses a minimum number of liens (only necessary ones). Make sure that the top rule and bottom rule (top and bottom horizontal lines) of a table are present.

Table 4.1: Example of a table in LaTeX

Bike		
Type	Color	Price (£)
Electric	black	700
Hybrid	blue	500
Road	blue	300
Mountain	red	300
Folding	black	500

4.3 Example of captions style

- The **caption of a Figure (artwork) goes below** the artwork (Figure/Graphics/illustration). See example artwork in Figure 3.1.
- The **caption of a Table goes above** the table. See the example in Table 4.1.
- The **caption of an Algorithm goes above** the algorithm. See the example in Algorithm 1.
- The **caption of a Listing goes below** the Listing (Code snippet). See example listing in Listing 3.1.

4.4 Summary

Write a summary of this chapter.

Chapter 5

Discussion and Analysis

Depending on the type of project you are doing, this chapter can be merged with "Results" Chapter as " Results and Discussion" as suggested by your supervisor.

In the case of software development and the standalone applications, describe the significance of the obtained results/performance of the system.

5.1 A section

Discussion and analysis chapter evaluates and analyses the results. It interprets the obtained results.

5.2 Significance of the findings

In this chapter, you should also try to discuss the significance of the results and key findings, in order to enhance the reader's understanding of the investigated problem

5.3 Limitations

Discuss the key limitations and potential implications or improvements of the findings.

5.4 Summary

Write a summary of this chapter.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

Typically a conclusions chapter first summarizes the investigated problem and its aims and objectives. It summaries the critical/significant/major findings/results about the aims and objectives that have been obtained by applying the key methods/implementations/experiment set-ups. A conclusions chapter draws a picture/outline of your project's central and the most signification contributions and achievements.

A good conclusions summary could be approximately 300–500 words long, but this is just a recommendation.

A conclusions chapter followed by an abstract is the last things you write in your project report.

6.2 Future work

This section should refer to Chapter 4 where the author has reflected their criticality about their own solution. The future work is then sensibly proposed in this section.

Guidance on writing future work: While working on a project, you gain experience and learn the potential of your project and its future works. Discuss the future work of the project in technical terms. This has to be based on what has not been yet achieved in comparison to what you had initially planned and what you have learned from the project. Describe to a reader what future work(s) can be started from the things you have completed. This includes identifying what has not been achieved and what could be achieved.

A good future work summary could be approximately 300–500 words long, but this is just a recommendation.

Chapter 7

Reflection

Write a short paragraph on the substantial learning experience. This can include your decision-making approach in problem-solving.

Some hints: You obviously learned how to use different programming languages, write reports in LaTeXand use other technical tools. In this section, we are more interested in what you thought about the experience. Take some time to think and reflect on your individual project as an experience, rather than just a list of technical skills and knowledge. You may describe things you have learned from the research approach and strategy, the process of identifying and solving a problem, the process research inquiry, and the understanding of the impact of the project on your learning experience and future work.

Also think in terms of:

- what knowledge and skills you have developed
- what challenges you faced, but was not able to overcome
- what you could do this project differently if the same or similar problem would come
- rationalize the divisions from your initial planed aims and objectives.

A good reflective summary could be approximately 300–500 words long, but this is just a recommendation.

Note: The next chapter is "**References**," which will be automatically generated if you are using BibTeX referencing method. This template uses BibTeX referencing. Also, note that there is difference between "References" and "Bibliography." The list of "References" strictly only contain the list of articles, paper, and content you have cited (i.e., refereed) in the report. Whereas Bibliography is a list that contains the list of articles, paper, and content you have cited in the report plus the list of articles, paper, and content you have read in order to gain knowledge from. We recommend to use only the list of "References."

Aspers and Corte (2019)

References

Altulaihan, E., Almaiah, M. and Aljughaiman, A. (2022), 'Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions', *Electronics* **11**(20).
URL: *https://doi.org/10.3390/electronics11203330*

Aspers, P. and Corte, U. (2019), 'What is qualitative in qualitative research', *Qualitative Sociology* **42**(2), 139–160.

Borgstede, M. and Scholz, M. (2021), 'Quantitative and qualitative approaches to generalization and replication–a representationalist view', *Frontiers in Psychology* **12**(1), 1–9.

Poornima, B. (2023), 'Cyber preparedness of the indian armed forces', *Journal of Asian Security and International Affairs* **10**(3), 301–324.
URL: *https://doi.org/10.1177/23477970231207250*
Borgstede and Scholz (2021)
Altulaihan et al. (2022)
Poornima (2023)

Appendix A

An Appendix Chapter (Optional)

Some lengthy tables, codes, raw data, length proofs, etc. which are **very important but not essential part** of the project report goes into an Appendix. An appendix is something a reader would consult if he/she needs extra information and a more comprehensive understating of the report. Also, note that you should use one appendix for one idea.

An appendix is optional. If you feel you do not need to include an appendix in your report, avoid including it. Sometime including irrelevant and unnecessary materials in the Appendices may unreasonably increase the total number of pages in your report and distract the reader.

Appendix B

An Appendix Chapter (Optional)

...