

SOLUTION ARCHITECTURE INFRASTRUCTURE SECURITY

INTERNSHIP

BY

AKIB ISTIAK RIFAT

ID: 213-15-4619

This Report Presented in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science in Computer Science and
Engineering

Supervised By

Mr. Dewan Mamun Raza

Assistant Professor

Department of CSE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

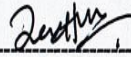
DHAKA, BANGLADESH

JANUARY 2025

APPROVAL

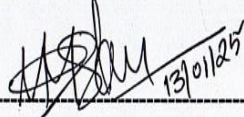
This Project titled “**Solution Architecture Infrastructure Security Internship**”, submitted by **Akib Istiak Rifat**, ID No: **213-15-4619** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **13 January, 2025**.

BOARD OF EXAMINERS



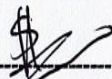
Dr. Md. Zahid Hasan
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Chairman



Mohammad Monirul Islam
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Mr. Afjal Hossan Sarower
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



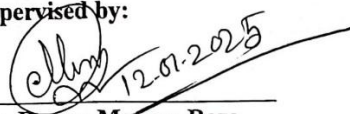
Dr. Ahmed Wasif Reza
Professor
Department of Computer Science and Engineering
East West University

External Examiner

DECLARATION

I hereby declare that this project has been done by us under the supervision of **Mr. Dewan Mamun Raza, Assistant Professor, Department of Computer Science and Engineering, Daffodil International University**. I also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:



Mr. Dewan Mamun Raza
Assistant Professor
Department of Computer Science and Engineering
Daffodil International University

Submitted by:



Akib Istiak Rifat
ID: 213-15-4619
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for His divine blessing making us possible to complete the final year project/internship successfully.

We are really grateful and wish our profound indebtedness to **Mr. Dewan Mamun Raza, Assistant Professor**, Department of CSE, Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “*Deep Learning*” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Sheak Rashed Haider Noori, Professor & Head**, Department of CSE, for his kind help to finish our project and also to other faculty members and the staff of CSE Department of Daffodil International University.

We would like to thank our entire course mates in Daffodil International University, who took part in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

During my internship at GO INNVOIR LTD, I was an intern focusing on security for infrastructure solutions. My main job was to keep the organization's computer security systems running and manage them. I worked hard to make sure our security was strong and that everything ran smoothly. I took care of Microsoft Office 365 by setting it up and improving it to fit our company's needs. I helped with cyber security by using forensic analysis methods to find and fix weaknesses. I used Kaspersky Cyber Security Solutions to improve the organization's ability to spot and handle threats. My work on improving Endpoint Detection and Response (EDR) made it easier to manage threats quickly. This means we can find and fix security problems faster. Along with these tasks, I did basic networking jobs to make sure that systems could talk to each other safely and effectively. In this job, I gained hands-on experience in setting up security measures, taking care of IT systems, and fixing security problems in a busy setting. During this internship, I learned important skills in computer security, managing IT systems, and networking. These experiences have helped me tackle real problems in business security design by focusing on preventing risks and making operations run smoothly.

Keywords: Cyber Security, Microsoft Office 365 Administration, Kaspersky Cyber Security, EDR Optimization, Networking, Forensic Analysis, IT Infrastructure, Security Architecture.

TABLE OF CONTENTS

| CONTENTS | PAGE |
|---|--------------|
| Board of Examiners | i |
| Declaration | ii |
| Acknowledgements | iii |
| Abstract | iv |
| CHAPTER | |
| CHAPTER 1: INTRODUCTION | 1-6 |
| 1.1 Introduction | 1 |
| 1.2 Motivation | 2 |
| 1.3 Internship Objective | 3-4 |
| 1.4 Introduction to the Company | 4-5 |
| 1.5 Report Layout | 5-6 |
| CHAPTER 2: BACKGROUND STUDY | 7-10 |
| 2.1 Introduction | 7 |
| 2.2 Mission and Vision | 8 |
| 2.3 SWOT Analysis | 9 |
| 2.4 Organizational Structure | 10 |
| CHAPTER 3: TASKS, PROJECTS, AND ACTIVITIES | 11-18 |
| 3.1 Daily Task and Activities | 11-13 |
| 3.2 Project Task and Activities | 13-17 |
| 3.3 Challenges | 17-18 |
| CHAPTER 4: COMPETENCIES AND SMART PLAN | 19-21 |

| | |
|--|--------------|
| 4.1 Competencies Earned | 19 |
| 4.2 Smart Plan | 20-21 |
| 4.3 Reflection | 21 |
| CHAPTER 5: OVERVIEW OF THE STUDY, CONCLUSION, AND FUTURE WORK | 22-24 |
| 5.1 Discussion and Conclusion | 22 |
| 5.2 Scoop for Future Career | 23 |
| 5.3 Future Work | 23-24 |
| REFERENCES | 25 |
| PLAGIARISM REPORT | 26 |

LIST OF FIGURES

| FIGURES | PAGE NO |
|---|----------------|
| Figure 2.1: Organization Structure | 10 |
| Figure 3.1: Cisco Router | 12 |
| Figure 3.2: Router and Switch from Data Center | 12 |
| Figure 3.3: Console cable | 13 |
| Figure 3.4: Meeting about Cyber Security Optimization | 14 |
| Figure 3.5: Network Architecture Diagram | 15 |
| Figure 3.6: Cybersecurity Workflow | 16 |
| Figure 3.7: EDR Optimization Process Diagram | 16 |
| Figure 3.8: Kaspersky Total Security | 17 |

CHAPTER 1

INTRODUCTION

1.1 Introduction

As an intern focusing on Solution Architecture Infrastructure Security at GO INNVOIR LTD, I am committed to learning and helping the company keep its cyber security and infrastructure strong. My main job is to keep the organization's technology safe and running smoothly. This job lets me use what I've learned in school and improve my skills in a real-world setting, helping me connect what I studied with how things work in businesses. In this job, I work on keeping online security strong and managing different computer systems to protect information and technology. I use Microsoft Office 365 to help people work together and be productive in a big organization. I also take care of cyber security and forensic tasks. This means I look for, investigate, and help reduce possible dangers to the organization's online assets. A big part of my job is using advanced tools like Kaspersky Cyber Security Solutions to improve protection for devices and make our Endpoint Detection and Response (EDR) systems work better. These tasks require careful attention and taking action early to fix problems quickly, which helps lower the chances of security issues. I also help with basic networking tasks to support the organization's systems and make sure everything communicates smoothly. This internship gives me a great chance to learn more about security, managing systems, and networking. By working on these tasks, I am improving my technical and problem-solving skills, getting ready for a fast-paced career in cyber security and infrastructure management.

1.2 Motivation

My motivation to pursue an internship in Solution Architecture Infrastructure Security at GO INNVOIR LTD stems from a strong passion for cybersecurity and system architecture. As technology continues to evolve, so do the challenges related to protecting information and infrastructure. I am driven by the desire to develop expertise in identifying, mitigating, and managing these threats, ensuring secure and efficient systems. The opportunity to work with advanced tools like Microsoft Office 365 administration, Kaspersky Cyber Security Solutions, and Endpoint Detection and Response (EDR) optimization aligns perfectly with my goal of gaining hands-on experience with cutting-edge technologies. These tools provide the foundation for learning about robust security protocols, enhancing administrative practices, and mastering forensic analysis—essential skills in today’s cybersecurity landscape. Another key motivator is the chance to apply theoretical knowledge to real-world scenarios. Through this internship, I am able to bridge the gap between academic learning and practical implementation, particularly in areas such as cyber forensic tasks, network security basics, and administrative processes. This experience equips me with the confidence to tackle complex challenges and make informed decisions in high-pressure situations. Furthermore, the dynamic and challenging environment at GO INNVOIR LTD allows me to work alongside industry experts and learn from their insights. This mentorship fosters personal growth, sharpens my technical acumen, and prepares me to contribute meaningfully to the field. I am motivated by the prospect of making a tangible impact on infrastructure security while continuing to evolve as a cybersecurity professional.

1.3 Internship Objective

The main goal of my internship at GO INNVOIR LTD as an Infrastructure Security professional is to learn more about cyber security and how to manage infrastructure. I want to use what I've learned in school in real-life situations and get practical experience with the latest tools and technologies. One of my main goals is to get better at keeping computer security safe and making it better. I am dedicated to finding weaknesses, putting strong solutions in place, and protecting the safety and privacy of the organization's data. Using tools like Kaspersky Cyber Security Solutions and EDR optimization helps me learn how to find and stop advanced online threats. By handling Microsoft Office 365 management, I am improving my ability to set up and keep big software running smoothly, which is important for good business operations. This also means knowing the details of managing user accounts and the security tools in the platform. Another important area is looking into cyber security crimes. I want to create a clear step-by-step way to find, study, and fix security problems. I am focused on learning the best ways to follow the rules and deal with legal issues. Basic networking tasks are an important part of my job. I am improving my skills in building, fixing, and improving network systems. My goal for this internship is to become better at creating, using, and managing safe IT solutions that deal with today's and tomorrow's problems in cyber security. I am excited to work with tools like Microsoft Office 365, Kaspersky Cyber Security Solutions, and Endpoint Detection and Response (EDR) because it will help me gain practical experience with the latest technologies. These tools help you learn about strong security rules, improve how things are managed, and understand how to investigate problems. These are important skills in today's world of cybersecurity. Another important reason is the opportunity to use what you learn in real-life situations. This internship helps me connect what I learned in school with real-world work, especially in things like cyber forensics, basic network security,

and office tasks. This experience gives me the confidence to handle difficult problems and make good choices when there is a lot of pressure. Also, the fast-paced and tough setting at GO INNVOIR LTD lets me work with experts in the field and learn from what they know. This mentorship helps me grow as a person, improves my skills, and gets me ready to make a real difference in my work. I am excited about the chance to help improve infrastructure security and grow as a cybersecurity expert. In this role, I make sure we follow cyber security rules and manage different technical systems to protect data and our infrastructure. I use Microsoft Office 365 to help teams work together and get things done better. I also take care of cyber security and forensic work. This means I look for, investigate, and reduce possible dangers to the organization's digital resources. A big part of my job is using advanced tools like Kaspersky Cyber Security Solutions to improve security for devices and make Endpoint Detection and Response (EDR) systems work better. These tasks need careful attention and an active way of working to quickly fix any weak points, which helps lower the chances of security problems. I help with simple networking tasks to support the organization's systems and make sure everything communicates smoothly. This internship gives me a great chance to learn more about security, managing systems, and networking. By working on these tasks, I am improving my technical and problem-solving skills, which will help me in a future job in cyber security and managing computer systems.

1.4 Introduction to the Company

The main goal of my internship at GO INNVOIR LTD as a Solution Architecture Infrastructure Security professional is to learn more about cyber security and managing infrastructure. I want to use what I've learned in school in a real-world

setting while getting practical experience with new technologies and tools. One of my main goals is to get better at keeping computer security rules and practices strong and effective. I am dedicated to finding weak points, putting strong solutions in place, and keeping the organization's data safe and private. Using tools like Kaspersky Cyber Security Solutions and EDR optimization helps me learn how to find and deal with serious online threats. By handling Microsoft Office 365 administration, I am improving my skills in setting up and keeping advanced software running, which is important for smooth business operations. This also means knowing the details of how to manage user accounts and safety features on the platform. Another important area I work on is investigating cyber security issues. I want to create a clear plan for finding, analyzing, and fixing security problems. I am committed to learning the best ways to follow the rules and deal with any legal issues. Basic networking tasks are an important part of my job. I am improving my skills in setting up, fixing, and making networks work better. My goal for this internship is to become better at creating, using, and managing safe IT solutions that solve today's and tomorrow's cyber security problems.

1.5 Report Layout

The distinctive features of our endeavors are as follows:

Chapter 1: The research topic's historical and contextual information is presented in the introduction, along with the investigation's challenge or query and the study's goals and relevance. This section includes the introduction of the paper in 1.1, the inspiration for the subject of the study in 1.2, the justification for the study's conduct in 1.3, the anticipated results of this article in 1.4, and the summary or format of the document in 1.5.

Chapter 2: An initial appraisal that provides a brief synopsis of the research conducted on this topic is included in the background study. The applicable intelligence technology research is described here. Moreover, the challenges we faced while doing this study demonstrated the size of the issue. The terminologies subsection is used to describe the areas we will investigate for the paper in 2.1, the related works that show the scientist's prior work in 2.2, the comparative evaluation and summary of the topic in 2.3, the overall goal of the paper in 2.4, and the difficulties we will encounter in 2.5.

Chapter 3: The main concepts of data set handling and model generation have been comprehensively covered in this section. In 3.1, the research approach is introduced; in 3.2, how the dataset is assembled; in 3.3, how the dataset is sterilized; in 3.4, the preliminary processing strategy of the dataset; and in 3.5 and 3.6, respectively, the recommended approach and the implementational prerequisites.

Chapter 4: This section assessed and looked into the output of our predictive framework. For ease of understanding, it incorporates all the results from the graphical description. This section comprises the evaluation of the paper and the experimental findings. The introductory part in 4.1, the result investigation in 4.2, the confusion matrix and classification report resemblance of the outcomes in 4.3 and 4.4, the precision of the validation and training in 4.5, and the discussion of the results segment in 4.6.

Chapter 5: The repercussions of marine life freshness on the community, the surroundings, as well as sustainability are briefly addressed in 5.1, 5.2, 5.3, and 5.4 accordingly.

Chapter 6: In accordance with 6.1, 6.2, and 6.3, an overview of the accomplished study, a conclusion, and potential future research are shown in this section.

CHAPTER 2

BACKGROUND STUDY

2.1 Introduction

GoInnovior Limited is a prominent IT service provider in Bangladesh, dedicated to delivering cutting-edge solutions across various industries. The company specializes in IT infrastructure, cybersecurity, business automation, IT consultancy, and digital marketing services. Established to empower organizations in the digital age, GoInnovior has gained a reputation for its expertise in transforming businesses into data-driven and technology-enabled enterprises. The organization provides an extensive range of services, including managed IT solutions, website development, domain and hosting, and technology training. Their consulting expertise extends to offering professional guidance for businesses to optimize their IT operations. With a strong emphasis on security, GoInnovior delivers robust cybersecurity measures, including endpoint detection and response (EDR), forensic analysis, and integrated cyber defense solutions. These services ensure data integrity and protection against evolving cyber threats. GoInnovior also stands out for its innovative solutions in modern workplace environments, blockchain technology, IoT, and web applications. The company collaborates with global partners such as Microsoft, Kaspersky, Cisco, and Fortinet to provide advanced IT services tailored to specific business needs. With over 500 satisfied clients, 200 completed projects, and 25 certified resources, GoInnovior has established itself as a trusted partner in the IT industry. Based in Dhaka, GoInnovior is committed to maintaining operational excellence and staying ahead in technology trends. Its mission is to provide scalable, reliable, and innovative IT solutions that empower businesses to achieve sustainable growth and success in a competitive digital landscape.

2.2 Mission and Vision

Mission

- I aim to provide cutting-edge IT solutions that empower businesses to achieve sustainable growth and adapt to the evolving digital landscape.
- I am dedicated to delivering scalable, secure, and innovative services tailored to meet client-specific needs.
- My focus is on building long-term partnerships by maintaining high standards of service quality, operational excellence, and customer satisfaction.
- I strive to enhance businesses' technological capabilities through expertise in cybersecurity, IT infrastructure, and automation.
- I am committed to fostering a data-driven and technology-enabled future for industries across various domains.

Vision

- I envision becoming a global leader in IT services by offering transformative and innovative solutions that drive business success.
- I aspire to set benchmarks in cybersecurity, IT consultancy, and digital transformation, ensuring organizations can operate securely and efficiently.
- I aim to lead in the adoption and integration of advanced technologies, including blockchain, IoT, and modern workplace solutions.
- I am determined to make technology education and accessibility available to all, promoting growth and digital literacy.
- I strive to create a digital ecosystem where businesses can thrive by leveraging reliable, scalable, and innovative IT solutions.

2.3 SWOT Analysis

Strengths:

- Strong expertise in IT infrastructure, cybersecurity, and business automation.
- Partnerships with leading global brands like Microsoft, Kaspersky, and Cisco.
- High client satisfaction with over 500 clients served.
- Proven track record of delivering innovative and reliable IT solutions.

Weaknesses:

- Dependence on external vendors for certain technology solutions.
- Limited geographic presence outside Bangladesh.

Opportunities:

- Expansion into international markets to reach a broader client base.
- Growing demand for advanced cybersecurity and digital transformation services.
- Potential for development of new services in emerging technologies like AI and blockchain.

Threats:

- Intense competition in the rapidly evolving IT industry.
- Continuous challenges related to cybersecurity risks and data breaches.

2.4 Organizational Structure

Phase-1: Project Preparation

- Initial planning and assessment of project requirements.
- Team formation and allocation of resources.
- Establishment of project goals and timelines.

Phase-2: Project Implementation

- Execution of planned strategies with close monitoring of progress.
- Coordination between departments for smooth workflow.
- Regular updates and adjustments based on project needs.

Phase-3: Operation of GoInnovior

- Continuous operation and maintenance of implemented solutions.
- Focus on customer support, cybersecurity, and system optimization.
- Regular assessment of performance metrics to ensure project success.

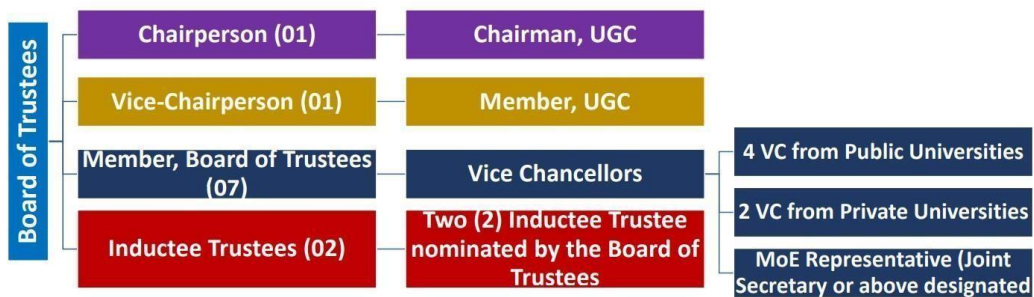


Figure 2.1: Organization Structure

CHAPTER 3

TASKS, PROJECTS, AND ACTIVITIES

3.1 Daily Task and Activities

During my internship at GoInnovior Limited as a Security intern, I spend my days keeping computers safe, doing office tasks, and improving IT systems. Every day, I check and take care of different security systems to keep the company safe from online dangers. I use tools like Kaspersky and EDR systems to watch for, find, and take care of possible security problems. One of my main jobs is managing Microsoft Office 365. I handle user accounts, set up security options, and make sure the system works well. This involves managing password changes, access rights, and fixing problems with Office 365 services. I also help with checking for security problems, looking into possible hacking cases, and reviewing the company's systems to make sure they are safe and working properly. I help find weaknesses and suggest ways to make security better. I also do simple networking jobs to make sure the company's network runs well and is safe. This involves fixing network problems, setting up routers, and keeping the internet working for different departments. In my daily work, I often work with my team to fix security problems and improve our systems. I go to meetings to learn about new security rules, what's happening in the industry, and new dangers. My job needs me to stay organized and to look out for possible problems that could harm the company's systems.



Figure 3.1: Cisco Router

The Cisco Router is a highly efficient networking device designed to manage and direct data traffic between computer networks. It enables seamless communication by routing data packets to their intended destinations, ensuring optimized performance and security. With advanced features, it supports scalability, secure connections, and reliable network operations in diverse environments.

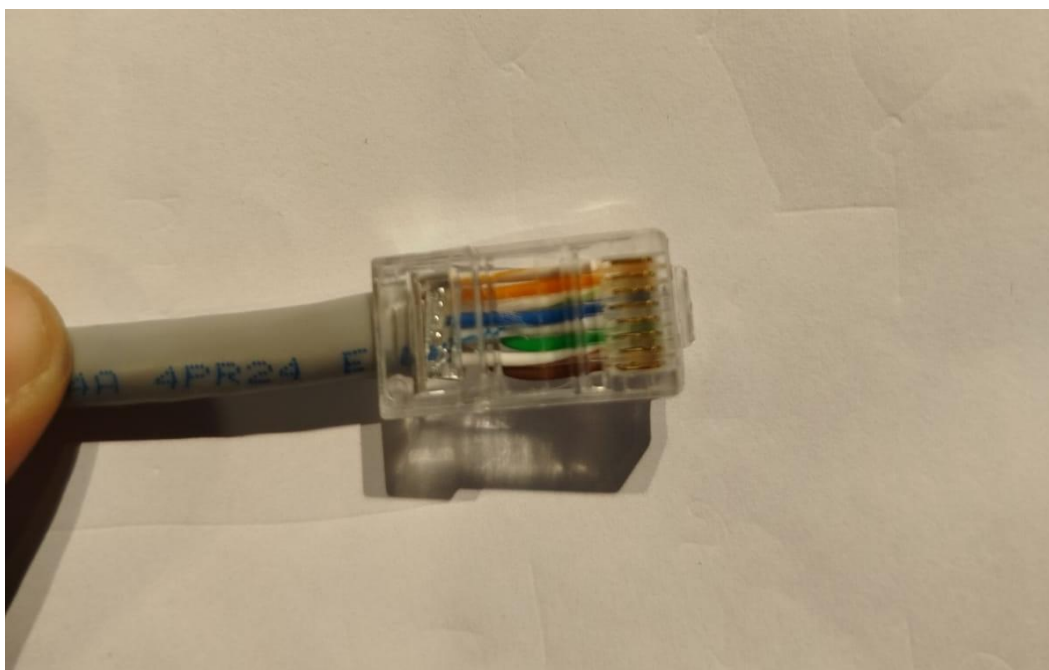


Figure 3.2: Cable with an RJ45 connector

This figure illustrates a router and switch setup in the data center, essential for ensuring efficient data routing, network connectivity, and seamless communication between devices within the infrastructure.



Figure 3.3: Console cable

3.2 Project Task and Activities

As a Security intern at GoInnovior Limited, my primary responsibilities involved protecting our computer systems, overseeing Microsoft Office 365, and enhancing our security tools. My job was to set up and oversee different security steps to keep the company's network and information safe. I helped set up and watch over security tools to stop possible dangers before they could do any damage. I helped take care of the organization's Microsoft Office 365. This included setting up user accounts, managing security rules, and fixing any problems with the system. My job also involved checking the endpoint detection and response (EDR) system to make sure it was working well at finding and reacting to possible cyber threats. I

took part in security checks and investigations, looking through records and checking for any unusual activities to make sure there were no security problems. Another important job was helping to set up and manage Kaspersky Cybersecurity Solutions. This included setting up different security measures and making sure the system stayed updated with the latest fixes and safety features. I also did simple networking tasks, like setting up network devices and fixing connection problems to help keep everything running well in the organization. During my internship, I worked with my team to make sure the security system was strong and met industry rules. I learned a lot by using cybersecurity tools and following best practices, which helped me improve my technical skills and knowledge of IT security management.



Figure 3.4: Meeting about Cyber Security Optimization

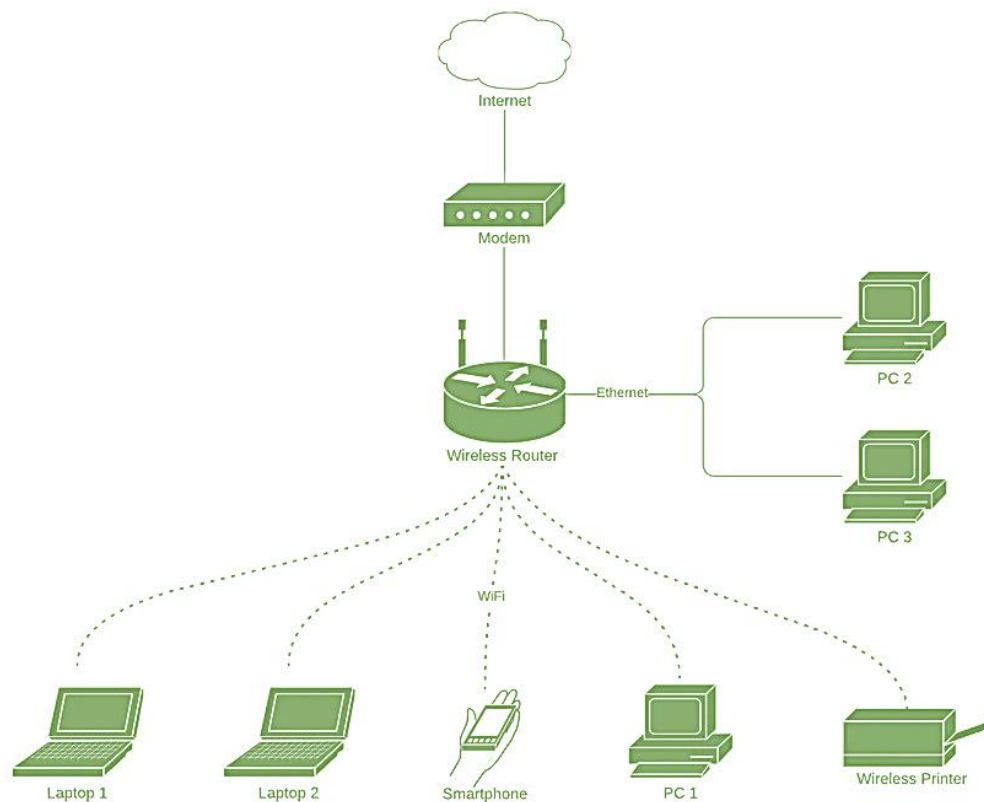


Figure 3.5: Network Architecture Diagram

The Network Architecture Diagram illustrates the structured layout of interconnected devices and systems within an organization. It highlights key components such as servers, firewalls, routers, switches, and endpoint devices. I ensure secure communication between network elements through optimized configurations, employing endpoint detection and response (EDR) solutions and firewalls. The diagram also emphasizes the integration of Microsoft Office 365 services, cloud storage, and on-premises systems, ensuring a seamless and secure flow of data within the infrastructure.

Cybersecurity Incident Response Workflow



Figure 3.6: Cybersecurity Workflow

The cybersecurity workflow involves identifying vulnerabilities, implementing security measures, monitoring systems, detecting threats, analyzing incidents, and responding to breaches. I ensure efficient processes by using tools like EDR, forensic analysis, and robust protection solutions to safeguard data.

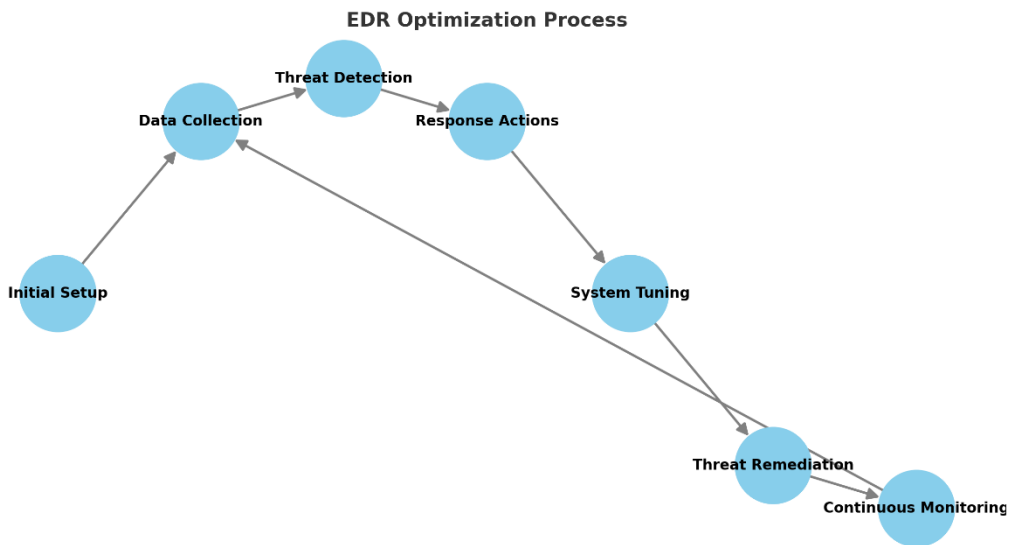


Figure 3.7: EDR Optimization Process Diagram

The diagram illustrates the EDR optimization process, focusing on threat detection, real-time response, and system performance enhancement. It highlights critical steps like data collection, threat analysis, remediation actions, and continuous monitoring to ensure robust cybersecurity.



Figure 3.8: Kaspersky Total Security

Kaspersky Total Security is an advanced cybersecurity solution that protects against viruses, malware, and online threats. It offers comprehensive features like password management, parental controls, and secure browsing to ensure data safety and user privacy effectively.

3.3 Challenges

I went through some difficulties that helped me grow as a person and in my job. One of the big challenges was dealing with how complicated the cybersecurity systems were. As an intern in the Security department, my job was to learn about and help manage the cybersecurity systems, including improving Endpoint Detection and Response (EDR) systems. This needed a deep understanding of different security methods and technologies, which was a bit confusing at first

because these tools are quite advanced. Another problem I faced was using Microsoft Office 365 administration. The platform has many features, like handling user accounts, security settings, and options. This required careful attention and a need to keep learning. Keeping up with changing internet safety risks meant we had to adjust quickly and solve problems fast. Also, using Kaspersky Cyber Security Solutions brought new difficulties in keeping an eye on and reacting to threats as they happen. The fast-changing threats meant I had to actively look for weaknesses and recommend ways to fix them. Finally, even though networking tasks were simple, I had to learn and use networking ideas quickly in real situations. Linking different security systems and making sure they work smoothly together on the company's network tested my technical skills. These challenges made me learn more about cybersecurity, get better at my technical skills, and adjust to the fast-moving IT environment at GoInnovior Limited.

CHAPTER 4

COMPETENCIES AND SMART PLAN

4.1 Competencies Earned

During my internship at GoInnovior Limited, I gained a lot of skills that improved my abilities in IT infrastructure and cybersecurity. I got hands-on experience in running and improving systems that detect and respond to security threats, making networks safer, and analyzing data for investigations. These tasks helped me see how important cybersecurity is for protecting sensitive information and stopping online threats. I learned how to use Microsoft Office 365. This includes managing who can access it, setting up security, and solving common problems. Also, my job at Kaspersky Cyber Security Solutions helped me learn more about advanced security methods, like finding threats, protecting against malware, and how to respond to incidents. By practicing basic networking tasks, I learned more about setting up networks, fixing problems, and connecting devices. I also learned about cloud technology, improving IT systems, and managing data. These are important for keeping businesses running smoothly and safely. I got better at communicating by working with different teams and talking about security plans and ways to make IT systems better. This experience helped me share useful ideas and learn from skilled workers. I learned about how to automate business tasks and use technology to make operations run more smoothly. This experience helped me see how technology can be used to make organizations work better and grow their business. Overall, my internship at GoInnovior Limited has given me the hands-on skills and understanding I need to tackle real problems in IT systems, online security, and digital solutions.

4.2 Smart Plan

The SMART Plan is a strategic approach designed to achieve specific goals with clarity, efficiency, and measurable outcomes. SMART stands for Specific, Measurable, Achievable, Relevant, and Time-bound. This methodology helps in setting clear objectives and tracking progress to ensure success in various projects and initiatives.

- **Specific:** The goals should be clearly defined and focused. In my role as a Solution Architecture Infrastructure Security intern, I aim to enhance the security infrastructure by implementing advanced cybersecurity measures, optimizing endpoint detection, and streamlining the administration of Office 365.
- **Measurable:** It is important to track progress and determine how success will be measured. For me, this includes improving security incident response times, optimizing EDR configurations, and increasing user engagement with security protocols. Success can be measured by the number of incidents detected and mitigated or by the time taken to resolve security breaches.
- **Achievable:** The goals must be realistic and attainable within the given resources and time. I will ensure that the tasks I set align with the available tools, training, and support from the organization, such as working with Kaspersky Cybersecurity Solutions and Microsoft Office 365.
- **Relevant:** The goals must align with the broader objectives of the company. Enhancing cybersecurity and optimizing IT infrastructure supports the organization's commitment to providing secure, reliable IT services to clients.
- **Time-bound:** A clear timeline is essential to ensure that the goals are achieved within a defined period. For instance, I plan to optimize the EDR

system within the next three months and complete the cybersecurity audit by the end of my internship.

By following this SMART Plan, I aim to contribute effectively to improving security protocols and IT infrastructure at GoInnovior Limited.

4.3 Reflection

I gained valuable hands-on experience in cybersecurity, IT infrastructure, and network management. I enhanced my skills in Microsoft Office 365 administration, forensic analysis, and endpoint detection response. This internship broadened my understanding of IT security and its critical role in business operations.

CHAPTER 5

OVERVIEW OF THE STUDY, CONCLUSION, AND FUTURE WORK

5.1 Discussion and Conclusion

My internship at GoInnovior Limited as a Solution Architecture Infrastructure Security intern, I learned a lot about the exciting world of cybersecurity and IT systems. My job included keeping our computer systems safe, managing Microsoft Office 365, improving security software, and doing some basic networking work. These tasks helped me see how important data security is and how complicated it can be to manage big IT systems. I got to use advanced cybersecurity tools like Kaspersky Cyber Security Solutions, which helped me understand how to find and respond to threats better. The forensic work helped me understand more about responding to incidents and why it is important to protect digital assets in a fast-changing environment with new threats. During my time at GoInnovior, I saw how the company's focus on being great at IT consulting, business automation, and digital marketing helps businesses succeed. The wide variety of services provided, like cloud computing and web apps, shows how the company can keep up with new technologies and what customers want. In conclusion, my internship at GoInnovior Limited was a valuable experience that allowed me to use what I learned in school in a real job. I now feel more sure about my skills to handle complicated computer systems and deal with security problems. The skills and knowledge I gained will definitely help me in my future jobs in IT and cybersecurity. This will allow me to make valuable contributions to the organizations I work for later on.

5.2 Scoop for Future Career

As I continue my journey in the field of IT infrastructure and cybersecurity, I see immense potential for growth and advancement. The rapid digital transformation across industries presents numerous opportunities for professionals like me to excel in diverse roles. With the increasing demand for secure and efficient IT systems, the scope for cybersecurity expertise is expanding, offering a broad range of career paths in areas like network security, ethical hacking, and cybersecurity management. The ongoing integration of advanced technologies such as cloud computing, artificial intelligence, and blockchain in business operations further enhances the scope for IT professionals. As I gain more expertise in these areas, I can contribute to the development of secure and scalable solutions, positioning myself as a valuable asset in any organization. Cybersecurity, in particular, continues to be a critical concern for businesses worldwide, making it a promising field with long-term career prospects. Additionally, the growing need for IT consultancy services across different sectors presents opportunities to work as a consultant, advising organizations on how to optimize their IT infrastructure and ensure robust cybersecurity measures. By acquiring more certifications and gaining hands-on experience, I can also progress into leadership roles such as Chief Information Security Officer (CISO) or Solutions Architect, where I would be responsible for shaping an organization's IT and security strategy. Overall, the future holds vast potential for me in IT infrastructure and cybersecurity, and I am excited to continue developing my skills and knowledge to take full advantage of the opportunities that lie ahead.

5.3 Future Work

In the future, I aim to further enhance my knowledge and skills in the field of architecture infrastructure and cybersecurity, particularly in the areas of cloud computing, automation, and advanced threat detection. The growing complexity of cyber threats calls for a deep understanding of emerging technologies and more sophisticated security protocols. I plan to continue expanding my expertise in these areas by pursuing additional certifications and training programs. Additionally, I will focus on improving my proficiency in operating and optimizing security tools like Kaspersky Cyber Security Solutions and Endpoint Detection and Response (EDR). As organizations increasingly adopt cloud-based infrastructures, I recognize the importance of mastering cloud security practices to protect sensitive data and ensure business continuity. I also aim to delve deeper into network security and forensic analysis to identify and mitigate potential vulnerabilities more effectively. Another key area of interest is expanding my knowledge of business automation and integrating AI-driven solutions into the IT infrastructure. By incorporating automation, I believe it will be possible to improve operational efficiency and response times in detecting and addressing security incidents. Through hands-on experience and further learning, I aim to contribute to the continuous improvement of GoInnovior's cybersecurity measures. I also aspire to take on more leadership responsibilities, managing larger-scale security projects and overseeing the implementation of new security architectures. By doing so, I will be able to support the organization in maintaining its high standards of cybersecurity while staying ahead of the evolving threat landscape.

REFERENCES

- [1] M. Abdullah, "An examination of the perceived need and recommended body of knowledge for architectural internship programs in Kuwait," OAKTrust Home, <https://oaktrust.library.tamu.edu/items/ad85154a-ecf6-4933-8683-3c875d51211c> (accessed Dec. 6, 2024).
- [2] A Textbook of Electrical Technology (Volume-II), <http://182.160.117.219:8080/xmlui/handle/123456789/110> (accessed Dec. 6, 2024).
- [3] C. Porumb *et al.*, "Virtual Laboratory and classware concepts in internship programmes," *2018 17th International Conference on Information Technology Based Higher Education and Training (ITHET)*, pp. 1–4, Apr. 2018. doi:10.1109/ithet.2018.8424807
- [4] C. Barros and N. Mateus-Coelho, "Detection and handling of threats in pre-established networks through a junior perspective in internship scenario," *ARIS2 - Advanced Research on Information Systems Security*, vol. 1, no. 1, pp. 41–49, Dec. 2021. doi:10.56394/aris2.v1i1.5
- [5] Digital Library Home: Hydraulics, Fluid Mechanics and hydraulic machines, <http://ir.juit.ac.in:8080/jspui/handle/123456789/5455> (accessed Dec. 6, 2024).
- [6] S. Chopvitayakun, "Android application to enhance performance of Internship Program Implementing Cloud Computing Platform and Infrastructure," *Procedia - Social and Behavioral Sciences*, vol. 197, pp. 2530–2538, Jul. 2015. doi:10.1016/j.sbspro.2015.07.617
- [7] Software product line (SPL) feature tree analysis tool, <http://103.133.167.5:8080/handle/123456789/2102> (accessed Dec. 6, 2024).
- [8] M. Jurgens and I. Helsloot, "The effect of social media on the dynamics of (self) resilience during disasters: A literature review," *Journal of Contingencies and Crisis Management*, vol. 26, no. 1, pp. 79–88, Nov. 2017. doi:10.1111/1468-5973.12212

- [9] Y. Ye, Q. Yu, Y. Zheng, and Y. Zheng, “Investigating the effect of social media application on firm capabilities and performance: The Perspective of Dynamic Capability View,” *Journal of Business Research*, vol. 139, pp. 510–519, Feb. 2022. doi:10.1016/j.jbusres.2021.10.008
- [10] K. Li *et al.*, “Dynamic probabilistic graphical model for progressive fake news detection on social media platform,” *ACM Transactions on Intelligent Systems and Technology*, vol. 13, no. 5, pp. 1–24, Jun. 2022. doi:10.1145/3523060

Plagiarism Report

ORIGINALITY REPORT

8%

SIMILARITY INDEX

6%

INTERNET SOURCES

5%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1

dspace.daffodilvarsity.edu.bd:8080

Internet Source

1%

2

Dr. Jason Edwards. "Critical Security Controls for Effective Cyber Defense", Springer Science and Business Media LLC, 2024

Publication

1%

3

jurnal.polines.ac.id

Internet Source

1%

4

Abdul Fadli Kalaloi, Alila Primayanti, Indria Angga Dianita, Gayes Mahestu, Pradipta Dirgantara. "Mediated Solidarity and Community Resilience on Twitter During Covid-19 Pandemic in Indonesia", 2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS), 2021

Publication

1%

5

Submitted to Georgia Military College

Student Paper

1%

6

aris-journal.com

Internet Source

1%