Quick Shield – A Smart Security System



EXECUTIVE SUMMARY

The rapid advancement of digital technology and the increasing use of laptops for academic, professional, and personal purposes have resulted in a rise in cyber threats such as hacking, malware infections, phishing attacks, and unauthorized access. Traditional antivirus software mainly relies on signature-based detection and usually responds only after an attack has already occurred, which makes systems vulnerable to modern threats.

To overcome this limitation, the project **"Quick Shield – A Smart Security System"** has been developed as a smart and proactive security solution for laptops. The system continuously monitors user activity and system behaviour to detect suspicious actions at an early stage.

Once a threat is identified, Quick Shield automatically takes protective actions such as disconnecting the internet, logging out active user sessions, locking sensitive files, and blocking unauthorized access. Additionally, the system uses a fake or decoy environment to confuse attackers, ensuring that the actual system and data remain completely safe.

Key Highlights of the Project:

- Detects hacking attempts in real time
- Automatically disconnects internet during an attack
- Logs out active user accounts for safety
- Locks sensitive files and folders instantly
- Uses a fake (decoy) environment to confuse attackers
- Protects the real system from data theft

Conclusion:

The study concludes that an active defense-based security system like Quick Shield offers better protection compared to traditional antivirus software. However, this project is developed as an academic model and can be further enhanced for commercial use with advanced AI and cloud-based security features.

Content

Chapter – 1 Introduction of Project **4 - 9**

- Background Of the Study 5
- Business Idea or Problem Statement 6
- Importance & Relevance 7
- Objectives 8
- Scope 9

Chapter – 2 Industry Profile / Literature Review **10-14**

- Overview of the Industry 11-12
- Market Size Growth Rate & Key Players 13
- Research and Literature 14

Chapter – 3 Industry Analysis **15-19**

- SWOT Analysis
  16-17
- PESTLE Analysis 18
- Emerging Technologies and Impact 19

Chapter – 4 Project Details **20-23**

- Market Plan 21
- Production Plan 22
- Financial Plan 23

Chapter – 5 Data Analysis and Findings **24-28**

- Data Collection and Methodology 25
- Analysis of Security Scenarios 26
- Findings and Interpretation 27-28

Chapter – 6 Conclusion **29-32**

Bibliography **33**

Appendices **33-35**

Chapter – 1 Introduction of Project

Introduction

1.1 Background of the Study

In today's digital age, laptops and computer systems play a vital role in academic, professional, and personal activities. With the increasing dependency on digital devices, the risk of cyber threats such as hacking, malware attacks, phishing, ransomware, and unauthorized access has also grown rapidly. Users store sensitive information like personal documents, academic records, financial data, and official work on their laptops, making them an attractive target for cybercriminals.

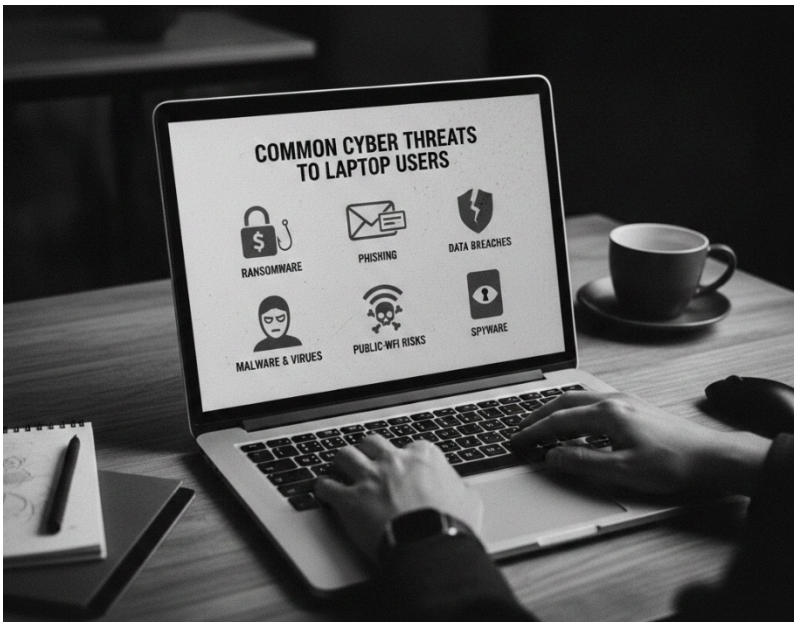
Most traditional antivirus software primarily relies on signature-based detection techniques. These systems are effective only against known threats and usually respond after an attack has already occurred. Modern cyberattacks are more sophisticated and often bypass conventional security systems by exploiting system behaviour, user mistakes, or zero-day vulnerabilities. As a result, users remain vulnerable despite having antivirus protection installed.

The core problem addressed in this project is the lack of a proactive, intelligent, and real-time security system for personal laptops. There is a need for a smart security solution that not only detects threats early but also takes immediate defensive action to prevent damage. The business idea behind **"Quick Shield – A Smart Security System"** is to overcome these limitations by introducing an active defense-based laptop security system that ensures data protection and system safety before serious harm occurs.

1.2 Business Idea and Problem Statement

The major problem in the current cybersecurity environment is the lack of a proactive and intelligent security solution for personal laptops. Existing antivirus systems mainly work in a reactive manner and fail to provide real-time protection against advanced and unknown cyber threats. This increases the risk of data theft, system damage, and privacy

violations for users.



The business idea behind **"Quick Shield – A Smart Security System"** is to develop an advanced laptop security solution that focuses on early threat detection and immediate defensive action. The system is designed to monitor system behaviour continuously and respond to suspicious activities in real time. Instead of waiting for damage to occur, Quick Shield aims to prevent cyberattacks at an early stage by isolating threats, protecting sensitive data, and ensuring system safety. This makes Quick Shield a smart, proactive, and reliable security solution for modern laptop users.

1.3 Importance and Relevance of the Innovative Idea

Cybersecurity has become one of the most important concerns in the modern digital environment. With the rapid growth of online education, remote working, digital payments, and cloud storage, individuals are increasingly exposed to cyber risks. Even a single security breach can lead to data loss, identity theft, financial damage, or privacy violations. Therefore, protecting personal devices such as laptops has become extremely important.

The relevance of **Quick Shield – A Smart Security System** lies in its proactive approach to cybersecurity. Unlike traditional antivirus software, which mainly focuses on virus removal, Quick Shield emphasizes real-time monitoring and prevention. The system is designed to detect suspicious behaviour at an early stage and take automatic actions to secure the system immediately.

This innovative idea is especially important for students, professionals, freelancers, and small business users who may not have access to expensive enterprise-level security solutions. Quick Shield provides a simple yet effective security mechanism that enhances user confidence while working online.

In the current scenario where cyber threats are continuously evolving, an active and intelligent security system is highly relevant. The concept of using a fake or decoy environment to mislead attackers further adds uniqueness and practical value to the project, making it suitable for present and future cybersecurity needs.

1.4 Objectives of the Project

The objectives of the project **"Quick Shield – A Smart Security System"** are formulated to address the growing cybersecurity challenges faced by laptop users. The primary objective is to design and propose a smart security system that provides real-time protection against various cyber threats.

One of the main objectives of this project is to study and understand the limitations of traditional antivirus software. By analyzing existing security solutions, the project aims to identify gaps where modern cyber threats are not adequately handled. Another important objective is to develop a proactive security mechanism that can detect suspicious activities based on system behaviour rather than only relying on known virus signatures.

The project also aims to implement automatic defensive actions such as internet disconnection, user session logout, file locking, and access restriction during a detected

threat. An additional objective is to introduce the concept of a fake or decoy environment that diverts attackers away from the actual system and data.

Furthermore, the project aims to ensure data safety, system integrity, and user privacy. The overall objective is to propose a user-friendly, reliable, and intelligent laptop security solution that can be further enhanced for commercial and large-scale use in the future.

1.5 Scope of the Project

The scope of the project **"Quick Shield – A Smart Security System"** is limited to the conceptual and academic development of a laptop security solution. The project focuses on studying cybersecurity threats, analyzing existing antivirus systems, and proposing an innovative and proactive security model for personal devices.

The system is designed specifically for laptops and personal computers used by students, professionals, freelancers, and small business users. The scope includes real-time threat detection, automatic response mechanisms, and the use of a decoy environment to protect the actual system. The project emphasizes behaviour-based monitoring rather than deep technical implementation of advanced hacking countermeasures.

As this is an academic mini project, the system is not developed for commercial deployment or enterprise-level usage. Certain advanced features such as large-scale cloud integration, real-time global threat intelligence, and full automation are outside the scope of this project.

However, the proposed model has strong potential for future enhancement. With additional resources and advanced technologies like artificial intelligence and cloud computing, the system can be expanded into a full-fledged commercial security product.

Chapter – 2
Industry Profile / Literature Review

2.1 Overview of the Selected Industry (Cybersecurity Industry)

The cybersecurity industry plays a crucial role in protecting digital systems, networks, and data from cyber threats. With the rapid growth of information technology, the use of computers, laptops, mobile devices, and the internet has increased significantly. As a result, the demand for cybersecurity solutions has also grown to safeguard sensitive information from unauthorized access, data breaches, and cyberattacks.

The cybersecurity industry includes various security solutions such as antivirus software, firewalls, intrusion detection systems, endpoint security, network security, and data protection tools. Initially, cybersecurity solutions were mainly developed for large organizations and enterprises. However, in recent years, the focus has shifted towards protecting personal devices such as laptops and home systems due to the rise in cybercrime targeting individual users.



The industry is continuously evolving to address new and complex threats like ransomware, phishing attacks, zero-day vulnerabilities, and social engineering attacks. Traditional security systems are gradually being replaced or enhanced with advanced technologies such as artificial intelligence, machine learning, and behavior-based detection.

The project **"Quick Shield – A Smart Security System"** is positioned within the personal and endpoint security segment of the cybersecurity industry. It aims to provide a proactive and intelligent security solution specifically designed for laptop users, making it relevant to the current and future needs of the cybersecurity market.

2.2 Market Size, Growth Rate, and Key Players

The global cybersecurity market has witnessed rapid growth over the past decade due to increasing cyber threats and digital transformation across industries. According to various industry reports, the global cybersecurity market is valued at hundreds of billions of dollars and is expected to grow at a strong compound annual growth rate in the coming years. Factors such as increased internet usage, cloud adoption, remote work culture, and digital payments have significantly contributed to this growth.

In the Indian context, the cybersecurity market is also expanding rapidly. With initiatives like Digital India, online education, and cashless transactions, the need for secure digital systems has increased. Both organizations and individual users are investing in security solutions to protect their data and privacy.

Some of the key players in the cybersecurity industry include companies such as **Quick Heal, Norton, McAfee, Kaspersky, Avast, Microsoft Defender, and Bitdefender**. These companies mainly provide antivirus and endpoint security solutions that focus on malware detection, firewall protection, and threat removal.

Despite the presence of many established players, there is still a gap in providing affordable, proactive, and behavior-based security solutions for personal laptop users. This gap creates an opportunity for innovative solutions like **Quick Shield – A Smart Security System**, which focuses on real-time protection and active defense mechanisms.

2.3 Review of Existing Research and Literature

Several research studies and academic papers have been published on cybersecurity, malware detection, and intrusion prevention systems. Most of the existing literature highlights the limitations of traditional signature-based antivirus systems, especially in detecting unknown and advanced cyber threats. Researchers have pointed out that modern cyberattacks often exploit user behavior and system vulnerabilities rather than relying on known malware signatures.

Many studies emphasize the importance of behavior-based detection techniques, which analyze system activities such as unusual file access, unauthorized login attempts, and abnormal network behavior. Artificial intelligence and machine learning have been widely discussed in recent literature as effective tools for improving threat detection accuracy and reducing false positives.

Another important area of research is deception technology, which involves the use of honeypots or decoy systems to confuse attackers and protect real assets. Although deception techniques are mainly used in enterprise-level security systems, recent studies suggest that such approaches can also be effective for personal device protection.

The literature review indicates that while advanced security techniques exist, they are rarely implemented in simple and affordable solutions for individual laptop users. The project **"Quick Shield – A Smart Security System"** is aligned with these research findings, as it combines behavior-based monitoring with deception techniques to provide an innovative and proactive security solution.

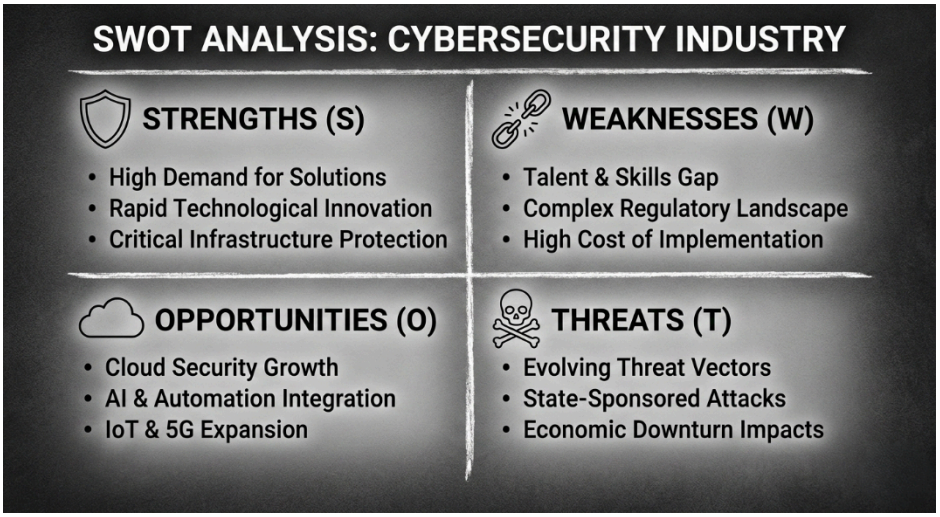
Chapter – 3
Industry Analysis

Analysis using frameworks like SWOT, PESTLE, or Porter's Five Forces.

3.1 SWOT Analysis of the Cybersecurity Industry

SWOT analysis is an important strategic tool used to analyze the internal strengths and weaknesses, as well as the external opportunities and threats faced by an industry. In the context of the cybersecurity industry, SWOT analysis helps in understanding the overall position and growth potential of security solutions such as antivirus and smart security systems.

The **strengths** of the cybersecurity industry include the increasing dependence on digital technologies and the growing awareness about data protection and privacy. Cybersecurity solutions are now considered essential rather than optional. Continuous technological advancements and innovation further strengthen this industry.



The **weaknesses** include the high cost of advanced security solutions and the complexity of implementation for non-technical users. Many individuals still lack proper knowledge of cybersecurity practices, which reduces the effective use of security tools.

The **opportunities** in this industry are significant due to the rise in cybercrime, remote working culture, online education, and digital payments. There is a growing demand for affordable and user-friendly security solutions for personal devices, which creates scope for innovative products like **Quick Shield – A Smart Security System**.

The **threats** include rapidly evolving cyberattack techniques, intense competition among existing players, and the challenge of keeping security solutions updated against new threats.

3.2 PESTLE Analysis of the Cybersecurity Industry

PESTLE analysis is used to evaluate the external macro-environmental factors that influence an industry. The cybersecurity industry is highly affected by political, economic, social, technological, legal, and environmental factors.

Political factors include government policies related to data protection, cybersecurity laws, and national digital security initiatives. Governments across the world are focusing on strengthening cybersecurity frameworks, which positively impacts the industry.

Economic factors such as increased digital transactions, e-commerce growth, and remote work culture have increased the demand for cybersecurity solutions. However, economic slowdowns may reduce spending on premium security products.

Social factors involve increasing awareness of cyber threats among users. People are becoming more concerned about data privacy, identity theft, and online fraud, which encourages the adoption of security systems.

Technological factors play a major role in this industry. Advancements in artificial intelligence, machine learning, and cloud computing have transformed cybersecurity solutions, making them smarter and more efficient.

Legal factors include compliance with data protection laws and regulations. Companies must ensure that their security solutions meet legal standards.

Environmental factors have limited direct impact, but the shift toward digital systems reduces paper usage and supports sustainability.

3.3 Emerging Technologies and Their Impact on the Industry

Emerging technologies are significantly transforming the cybersecurity industry by improving threat detection, response time, and overall system efficiency. One of the most impactful technologies is **Artificial Intelligence (AI)**, which enables security systems to analyze large volumes of data and identify suspicious patterns in real time.

Machine Learning (ML) allows cybersecurity solutions to learn from past incidents and improve detection accuracy over time. Behavior-based detection systems powered by ML can identify unknown threats that traditional signature-based antivirus software often fails to detect.

Another important emerging technology is **deception technology**, which involves the use of fake systems or decoy environments to trap attackers. This approach not only protects real data but also helps in understanding attacker behavior. Although mainly used in enterprise security, deception techniques are gaining attention for personal device protection.

Cloud-based security solutions are also becoming popular as they allow centralized threat intelligence and faster updates. Additionally, automation and real-time monitoring tools help reduce manual intervention and improve response efficiency.

The project **"Quick Shield – A Smart Security System"** aligns with these emerging trends by adopting behavior-based monitoring and deception techniques, making it a future-ready solution in the cybersecurity industry.

Chapter – 4
Project Details

4.1 Market Plan

(Target Customers, Market Analysis, and Marketing Strategies)

The market for cybersecurity solutions has expanded rapidly due to the increasing number of cyber threats and the growing dependence on digital devices. The target customers for **Quick Shield – A Smart Security System** primarily include students, working professionals, freelancers, remote workers, and small business owners who use laptops for daily activities and store sensitive data on their systems.

Students require security to protect academic data, projects, and personal information, especially while using public Wi-Fi networks. Professionals and freelancers need protection for confidential work files and client data. Small businesses also require affordable security solutions to safeguard employee laptops without investing in costly enterprise-level systems.

The market analysis indicates that while many antivirus products are available, most focus on basic virus detection and lack proactive defense mechanisms. There is a clear demand for a smart, real-time security system that can actively prevent attacks rather than only responding after damage occurs.

The marketing strategy for Quick Shield would focus on highlighting its unique features such as real-time threat detection, automatic system protection, and decoy environment technology. Online marketing, educational campaigns, free trial versions, and partnerships with educational institutions can be effective strategies to reach the target audience and create awareness.

4.2 Production Plan

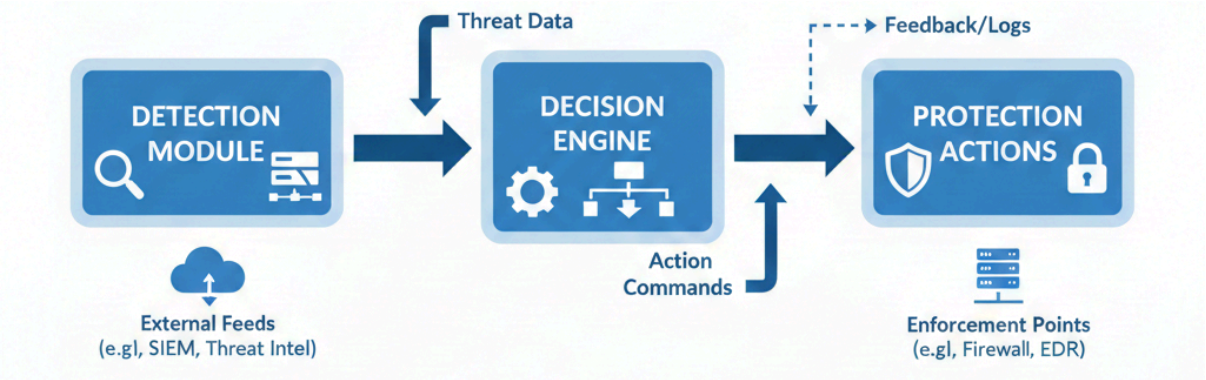
(Product Development, Required Resources, and Location)

Quick Shield – A Smart Security System is a software-based product designed for laptop security. The production of this system mainly involves software development rather than physical manufacturing. The development process includes system design, coding, testing, and deployment of the security application.

The required resources for producing Quick Shield include skilled human resources such as software developers, cybersecurity analysts, and testers. Development tools such as programming languages (Python, Java, or C++), security frameworks, and testing environments are also essential. In addition, basic hardware resources like development laptops, secure servers for testing, and cloud storage for backup may be required.

The production location for Quick Shield does not require a physical factory, as the entire development process can be carried out in a software development environment. The system can be developed remotely using collaborative tools, making it cost-effective and flexible.

Testing plays a crucial role in the production plan to ensure that the system performs well against various cyber threats. Regular updates and improvements are also necessary to maintain effectiveness. Since this project is developed as an academic model, the production scope is limited; however, the same framework can be scaled for commercial deployment in the future.



4.3 Financial Plan

(Cost Estimation and Proposed Selling Price)

The financial plan for **Quick Shield – A Smart Security System** focuses on estimating the total cost required for developing, launching, and operating the software as a commercial security product. Since Quick Shield is a software-based system, the major expenses are related to human resources, development tools, cloud infrastructure, and operational activities rather than physical production.

The **development cost** includes expenses for software design, programming, cybersecurity research, system testing, and quality assurance. For building a market-ready product, this cost is estimated at approximately **₹60–80 lakh** (around **USD 72,000–96,000**). This includes salaries for developers, security analysts, and testers, along with the use of development platforms and testing tools. Additional **infrastructure costs**, such as cloud servers, data storage, and licensed security tools, may require around **₹25–30 lakh** (USD 30,000–36,000).

The **operational cost** involves system maintenance, regular updates, customer support, and administrative expenses, estimated at **₹10–15 lakh** annually. **Marketing and promotional activities**, including digital marketing, branding, and customer acquisition, may require an additional **₹20–25 lakh**.

Overall, the **total estimated cost to start the company** is approximately **₹1.2 crore to ₹1.5 crore**, which is equivalent to **USD 140,000 to USD 180,000 (approx.)**.

To ensure affordability and steady revenue, a **subscription-based pricing model** is proposed. The suggested selling price is **₹499 per year for individual users** and **₹999 per year for professional users**, making Quick Shield a cost-effective and scalable security solution with strong market potential.

Chapter – 5
Data Analysis And Findings

5.1 Data Collection and Methodology

Since **Quick Shield – A Smart Security System** is an innovative and conceptual security project, the data used for analysis is primarily based on **secondary sources** and **simulated use-case scenarios** rather than real-time field data. Primary data collection in the form of live cyberattack logs or real user attack records is not feasible at the academic project level. Therefore, this project relies on existing cybersecurity reports, research papers, industry articles, and documented case studies related to laptop security and antivirus performance.

The data collection process involved studying common cyber threats faced by laptop users such as malware infections, phishing attacks, unauthorized access attempts, and suspicious system behaviour. Information was also gathered from comparative studies of traditional antivirus software to understand their strengths and limitations. In addition, hypothetical scenarios were created to analyze how Quick Shield would respond during different types of security threats.

This methodology helps in evaluating the effectiveness of a proactive security system without performing real attacks. The collected data was organized in a descriptive format and interpreted logically to support the objectives of the project. This approach ensures that the analysis remains realistic, ethical, and suitable for an academic study.

5.2 Analysis of Security Scenarios

The analysis of simulated security scenarios provides valuable insights into the functioning of **Quick Shield – A Smart Security System**. Various threat situations such as phishing link access, unauthorized login attempts, malicious USB insertion, and suspicious background processes were considered during the analysis. These scenarios represent common risks faced by laptop users in real-life situations.

The analysis shows that traditional antivirus systems often fail to respond immediately to such threats, especially when the attack does not involve known malware signatures. In contrast, Quick Shield focuses on behaviour-based monitoring, allowing it to identify unusual system activities at an early stage. Once a threat is detected, the system activates protective actions such as disconnecting the internet, logging out active user sessions, locking sensitive files, and blocking further access.

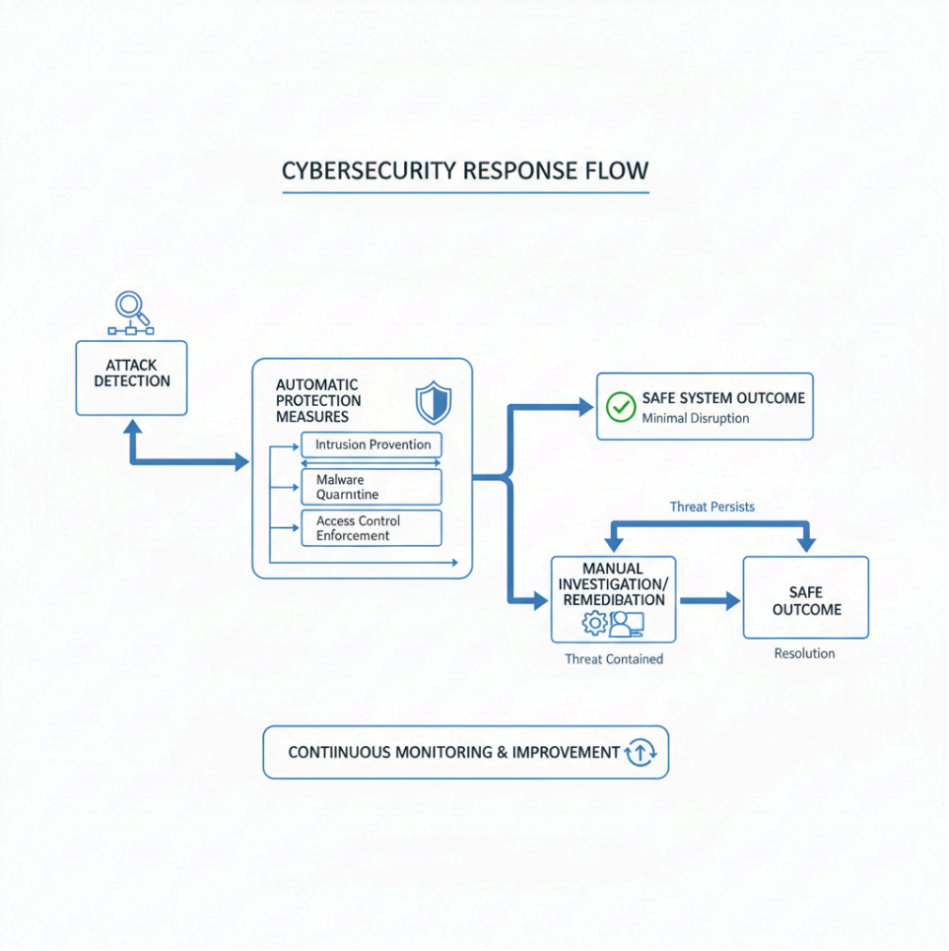
Another important observation from the analysis is the effectiveness of the fake or decoy environment. By redirecting attackers to a controlled environment, Quick Shield prevents them from accessing the actual system and sensitive data. This approach significantly reduces the risk of data theft and system damage.

Overall, the scenario analysis indicates that an active defense-based security system provides stronger protection compared to reactive antivirus solutions.

5.3 Findings and Interpretation

Based on the data analysis and simulated security scenarios, several key findings were identified. One of the major findings is that most cyber threats target user behaviour and system vulnerabilities rather than relying solely on malware files. This highlights the limitation of signature-based antivirus systems and the importance of behaviour-based security mechanisms.

The findings suggest that **Quick Shield – A Smart Security System** can enhance laptop security by responding to threats in real time. Automatic actions such as system lockdown, session logout, and file protection help minimize the impact of an attack. The use of a decoy environment further strengthens security by confusing attackers and diverting them away from real data.



Another important finding is that users benefit from reduced dependency on manual security actions. Quick Shield operates automatically, reducing the chances of human error during a cyberattack. This makes the system suitable for non-technical users as well.

However, the findings also indicate that the system's effectiveness is based on conceptual assumptions and simulated conditions. Real-world deployment would require advanced testing, continuous updates, and integration with external threat intelligence sources. Despite these limitations, the findings support the feasibility and relevance of Quick Shield as a smart laptop security solution.

Chapter – 6
Conclusion

CONCLUSION

The project **"Quick Shield – A Smart Security System"** was undertaken to study the growing cybersecurity threats faced by laptop users and to propose an innovative and proactive security solution. With the increasing use of digital devices for education, work, and personal activities, the risk of hacking, malware, phishing, and unauthorized access has also increased significantly. Traditional antivirus software mainly works on signature-based detection and usually reacts after an attack has already occurred, which makes them less effective against modern cyber threats.

This project highlights the importance of adopting a smart and active defense approach to laptop security. Quick Shield is designed to monitor system behaviour continuously and respond to suspicious activities in real time. Features such as automatic internet disconnection, session logout, file locking, and the use of a fake or decoy environment help protect the actual system and sensitive data from attackers. The project demonstrates that behaviour-based detection and deception techniques can enhance security beyond conventional antivirus solutions.

The findings of this study indicate that Quick Shield can serve as an effective and user-friendly security solution for students, professionals, freelancers, and small business users. However, since this project is developed as an academic and conceptual model, further development, real-world testing, and advanced implementation would be required for commercial deployment. Future improvements may include advanced artificial intelligence, cloud-based threat intelligence, and enterprise-level security features to make the system more robust and scalable.

FEASIBILITY ANALYSIS

(Quick Shield – A Smart Security System)

The feasibility analysis of Quick Shield – A Smart Security System is conducted to evaluate whether the proposed project is practical, achievable, and sustainable from different perspectives. The analysis includes technical feasibility, economic feasibility, operational feasibility, and market feasibility.

1. Technical Feasibility

Quick Shield is a software-based security system, and its development is technically feasible using existing technologies. The system can be developed using commonly available programming languages, cybersecurity frameworks, and cloud platforms. Features such as behaviour-based monitoring, system activity tracking, and automatic protection actions are already supported by modern operating systems and security tools. Since the project does not require any specialized hardware, it can be implemented on standard laptops and systems. Therefore, the project is technically feasible at both academic and commercial levels.

2. Economic Feasibility

From an economic point of view, Quick Shield is feasible as it can be developed using open-source tools and a small development team. The estimated startup cost can be managed within a reasonable budget, especially in a bootstrapped or student startup model. The proposed subscription-based pricing model (₹499–₹999 per year) makes the product affordable for users while ensuring continuous revenue for maintenance and updates. Hence, the project is economically viable.

3. Operational Feasibility

The system is designed to be user-friendly and operates automatically in the background without requiring technical knowledge from users. This makes it suitable for students, professionals, and small businesses. Minimal user intervention is required, which increases acceptance and ease of use. Therefore, the project is operationally feasible.

4. Market Feasibility

With the rising number of cyber threats and increasing dependence on laptops, there is strong demand for affordable and smart security solutions. The lack of proactive security systems for individual users creates a market opportunity for Quick Shield. Hence, the project is market feasible.

Bibliography

- Stallings, W. (2019). Network Security Essentials: Applications and Standards. Pearson Education.
- Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.
- Kumar, S., & Singh, A. (2020). Cyber security challenges and solutions for modern systems. International Journal of Computer Applications, 176(12), 15–20.
- National Institute of Standards and Technology (NIST). (2022). Cybersecurity Framework. https://www.nist.gov/cyberframework
- Kaspersky Lab. (2023). Endpoint Security Overview. https://www.kaspersky.com
- Quick Heal Technologies. (2023). Understanding Antivirus and Endpoint Protection. https://www.quickheal.com
- Symantec Corporation. (2022). Internet Security Threat Report. https://www.broadcom.com
- Kaspersky Lab. (2023). Cybersecurity resource center. https://www.kaspersky.com/resource-center
- Cisco Systems. (2023). What is cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Appendices

Appendix A: Cost Breakup of Quick Shield – A Smart Security System

This appendix shows the **actual estimated cost breakup** for developing and launching **Quick Shield – A Smart Security System** as a commercial software product. Since it is a software-based system, there is **no physical production cost** involved.

Estimated Cost Details:

- **Software Development Cost:**
  (Programming, testing, security research)
  ₹60–80 lakh
- **Infrastructure & Technology Cost:**
  (Cloud servers, data storage, licensed tools)
  ₹25–30 lakh
- **Operational Cost:**
  (Maintenance, updates, customer support)
  ₹10–15 lakh
- **Marketing & Promotion Cost:**
  (Digital marketing, branding, promotions)
  ₹20–25 lakh

Total Estimated Startup Cost:

₹1.2 crore – ₹1.5 crore
(USD 140,000 – USD 180,000 approx.)

These costs provide a clear understanding of the financial requirement needed to start the company.

Appendix B: Pricing Model

Quick Shield follows a **subscription-based pricing model** to make the product affordable and easy to use.

- **Individual Users:** ₹499 per year
- **Professional Users:** ₹999 per year

This pricing strategy helps in attracting users while ensuring regular revenue for updates and support.

Appendix C: Key Assumptions

- Costs are estimated for initial launch phase
- Open-source tools are partially used
- Small development team assumed
- Actual cost may vary based on market conditions