A MODEL FRAMEWORK FOR MANAGING CYBER SECURITY CHALLENGES FACED BY CLOUD-BASED SMALL IT FIRMS

Munasinghe Arachchige Nadeesha Tharika Sewwandi

219406J

MSc in Computer Science Specialising in Security Engineering

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

May 2025

A MODEL FRAMEWORK FOR MANAGING CYBER SECURITY CHALLENGES FACED BY CLOUD-BASED SMALL IT FIRMS

Munasinghe Arachchige Nadeesha Tharika Sewwandi

219406J

Thesis/Dissertation submitted in partial fulfillment of the requirements for the degree MSc in Computer Science Specialising in Security Engineering

Department of Computer Science and Engineering
Faculty of Engineering

University of Moratuwa
Sri Lanka

May 2025

DECLARATION

I declare that this is my own work and this thesis/dissertation does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other University or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. I retain the right to use this content in whole or part in future works (such as articles or books).

27/05/2025

Signature: Date:

The above candidate has carried out research for the Masters thesis under my supervision. I confirm that the declaration made above by the student is true and correct.

Name of Supervisor: Prof. Shantha Fernando

Signature of the Supervisor: Date: 2025-05-27

ACKNOWLEDGEMENT

I would like to acknowledge and express my sincere gratitude to the following individuals who supported me to make this work possible. Their direction and advice carried me through all the stages of writing my project.

I am grateful to University of Moratuwa, Sri Lanka for providing me with the necessary resources and facilities to complete this project.

My supervisor, Dr. Shantha Fernando, for providing the valuable guidance and response throughout the course of my research.

I am grateful to all the small IT firms who send their valuable responses to complete this project.

Last but not least, I have to mention the care and encouragement of my family and friends. Their support was invaluable throughout my studies.

ABSTRACT

Security threats and other cyber security-related concerns are becoming more prevalent in the business world. Small-to-medium-sized organizations are frequently targeted by attackers, and some find it challenging to withstand such attacks. Due to a lack of experience and the high cost of security solutions, small IT firms frequently encounter difficulties when setting up and implementing security measures. Hence, small IT firms and its stake holders are required to acknowledge the risk of cyber threats and continue their businesses without having a proper solution for their security related issues. The researcher conducted a comprehensive survey that focuses on the requirement of technical implementation of several cyber security controls for cloud-based small IT firms in accordance with this particular research. The survey encompassed a range of questions including existing cloud security controls, policies and procedures, access control and authentication mechanisms, cryptographic controls, password security, employee security awareness, incident response, security assessments and digital forensic, which helps to identify and understand overall organizations' operational structure and its business environment with the requirement for cybersecurity. The survey was sent to the small IT firms who is handling healthcare business systems and the small IT firms who is handling retail business systems. The information collected was thoroughly reviewed and visualized to identify security related challenges for cloud based small IT firms. Based on the identified security requirements of different kind of businesses, a framework was implemented to build small IT firms' security infrastructure using feasible open-source solutions. The most suitable open-source solutions were selected based on the type of the organization, types of the data collected, existing IT infrastructure, etc. The attributes of the framework ought to be cost effectiveness and user friendliness.

Keywords: Small IT firms, Cyber Security Framework, Open-source tools for Cyber Security

TABLE OF CONTENTS

LIST OF FIGURES

Figure **Description** **Page**

LIST OF TABLES

Table **Description** **Page**

LIST OF ABBREVIATIONS

Abbreviation	Description
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASD	Australian Signals Directorate
C5	Cloud Computing Compliance Control Catalog
CI/CD	Continuous Integration and Continuous Deployment
COVID-19	Coronavirus disease 2019
CPU	Central Processing Unit
CSA Cloud Controls Matrix (CCM)	Cloud Security Alliance Cloud Controls Matrix
FedRAMP	Federal Risk Authorization Management Program
GB	Giga Byte
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HIPAA	Health Insurance Portability and Accountability Act
HMAC	Hash-based Message Authentication Code
HR	Human Resources
HTTPS	Hyper Text Transfer Protocol Secure
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ISO/IEC 27001	International Organization for Standardization/ International Electrotechnical Commission 27001
IT	Information Technology
JWT	Json Web Token
MFA	Multi Factor Authentication
ML	Machine Learning
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework

NIST SP 800-53	National Institute of Standards and Technology Special Publication 800-53
NISTIR 7621	National Institute of Standards and Technology Interagency Report 7621
OS	Operating System
OSINT	Open-Source Intelligence
PCI DSS	Payment Card Industry Data Security Standard
PCI DSS	Payment Card Industry Data Security Standard
RAM	Random Access Memory
RBAC	Role Based Access Control
SIEM	Security Information and Event Management
TLS	Transport Layer Security
VM	Virtual Machine
VPN	Virtual Private Network
WAF	Web Application Firewall
Wi-Fi	Wireless Fidelity

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1. Background

Due to variances in resources, complexity and goals, small IT firms and large IT corporations often take distinct approaches to secure IT infrastructure [1]. Large IT organizations frequently have resources and a larger IT security team, enabling them to put in place a thorough IT security infrastructure that includes complex firewalls, IDS, IPS, encryption tools, SIEM systems, other security controls and tools [26]. Small IT firms frequently lack enough IT security resources and may be forced to rely on simple security measures like antivirus software, firewalls, and passwords. Additionally, they can have a smaller IT security team, which could affect their capacity to set up and manage sophisticated security solutions. When comparing the risk profiles of small IT firms against large businesses, small IT firms are more vulnerable to cyberattacks due to lack of knowledge in security and security resources [1]. Hence, these small IT firms are being attacked more frequently because those are considered as easy targets by hackers [4]. During the year 2022, 61% of small businesses including IT firms had to face cyber-attacks and according to Business Australia 60% of them were not able to survive successfully after a cyberattack [21][22]. Figure 1 represents the graphical view of the impact of cyber attacks on small businesses including IT firms in 2022.

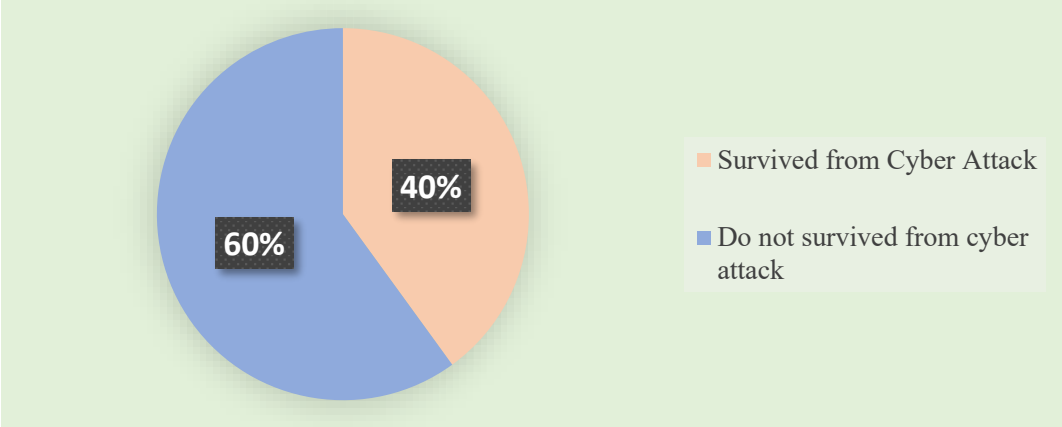


Figure 1: Impact of cyber-attacks on small businesses in 2022[21][22]

In the present, traditional computing infrastructure is considered as a costly solution and requires expertise knowledge for configuring and managing the entire organization in a secure manner [2]. Hence, most of the small IT firms are moving into cloud solutions due to its affordability, ease, scalability, and accessibility nature. Additionally, some of the security measures are already implemented in the existing cloud services [1]. The "Pay as you go," concept is popular among business entrepreneurs, which gives them the opportunity to lower the startup costs of their business. As a result, most of the business owners could launch their IT infrastructures of their businesses without giving much effort. With the COVID-19 pandemic, most of the small IT firms (IT organizations) started following work-from-home or hybrid methods for their employees. Hence, these employees started accessing their systems using the public internet. As the use of cloud environments grows, so do the cyber security risks associate with them [3].

Due to lack of resources and knowledge of cyber threats and secure configurations, even within the cloud environment, small IT firms could have gotten breached. According to Mahmoud Watad *et al*, some of the cyber security challenges that are for the small IT firms remain same for the cloud-based small IT firms [1].

Lack of employees with IT security knowledge and skills: The majority of small IT firms are not taking security of their IT infrastructure seriously. To protect the IT assets that are used for the company's operations, technical security expertise, cutting-edge security technologies and tools are required. Most of the small IT firms do not have IT security teams and other operational engineers may not have enough knowledge and skills to perform the security enhancements [1].

Misconfigurations: In the cloud environment, it is essential to change the default configurations to secure settings. Organizations must properly configure cloud-based security services when using them to protect their systems and data if they want to ensure that they are effective in lowering potential security threats. These security services can have vulnerabilities that an attacker could exploit if they are installed and configured incorrectly.

Expensiveness of Information Security: When initiating the process of securing small IT firms, starting from policies and procedure implementation, security expertise should identify the existing posture of the organization and build the security infrastructure. Thereafter, awareness programs, security assessments, security audits, etc. need to be performed regularly and updated according to the organizational changes. This process could be costly and security professionals may not be in the budget [1].

Insider Threats: Employees or third-party vendors who have access to the cloud infrastructure may intentionally or unintentionally expose sensitive data to unauthorized parties. This type of incidents may occur due to misconfiguration of the cloud services or stolen credentials. Hence, malicious actions could remain unnoticed due to lack of security controls in place [3]. Another aspect is, employees may use unauthorized software or hardware that may introduce new security risks. As a result of these, data breaches can occur.

Data Breaches: When sensitive data are stored and processed in the cloud environment, it makes them a desirable target for cybercriminals who want to access data without authorization by taking advantage of vulnerabilities in the cloud architecture. If such incident is occurred, sensitive data can be disclosed to the public internet.

Lack of Resources: In order to be protected from the cyber-attacks, large scaled organizations have sustainable resources when compared to the small IT firms. Most of the small IT firms only have fewer resources such as technologies, tools, etc.

1.2.Motivation and Research Problem

With the growth of cloud computing usage, cyber security attacks for small IT firms are increasing and the most of the business owners do not initiate security systems in their small IT firms. One of the main reasons for that is, starting a small IT firm requires a lot of time, effort, and resources, and many business owners may not

consider security as a critical aspect of their operations. They may be focused on other priorities such as generating revenue, acquiring customers, or developing products, and may not realize the importance of securing their business from cyber threats. However, failing to implement security can leave small IT firms vulnerable to a range of security risks, such as data breaches, malware attacks, and other cyber threats. As an example, small IT firms are facing cyber-attacks such as injection attacks, data structure attacks, path traversal, protocol manipulation, resource manipulation, sniffing attacks, embedded malicious code, etc. [2]. Such risks can result in financial losses, damage to the business's reputation, and other negative impacts on the business.

The Cyber security framework which is implemented by National Institute of Standards and Technology (NIST CSF) is frequently used by the small IT firms for implementing their cyber security posture [9]. NIST CSF could be used for initiating the security of the organization and identify the necessary security controls. ISO/IEC 27001 is another comprehensive framework that covers the entire information security management system (ISMS), including people, processes, and technology. ISO/IEC 27001 framework provides a set of controls and guidelines for establishing, implementing, maintaining, and continually improving an ISMS. CSA Cloud Controls Matrix (CCM) is providing the guidelines for cloud-based organizations to enhance the security. The security guidelines that are provided in the CCM, align with the security controls that are given in the frameworks such as PCI DSS, ISO 27001, ISO 27002, and NIST SP 800-53. All these standard frameworks provide in-depth guidelines and yet, technical implementation of these controls may not be affordable for the small- scale businesses. Most of these cyber security frameworks that are already exists, require expert knowledge to implement those in their environment and require costly tools and services.

The security tools and services that are designed for the enterprise level organizations, does not provide an affordable version for small-scaled businesses. Hence, most of the small-scale businesses are unwilling to buy costly and popular software/hardware solutions that are available in the market. For protecting cloud-based small-scale businesses from cyber-threats, an affordable cyber security framework, which could

perform technical support for improving the security posture of the organization, is required. Even without an expertise knowledge, those tools should be simple to use.

As explained in the previous sections, still cloud based small IT firms are remain exposed due to lack of knowledge and less expensive resources in cyber security. Most of them are unaware about possible open-source solutions that could be used to level up their security of the business. And even if they are aware about those open-source solutions, they may struggle to find the best and suitable security solutions for their business, according to their business type. Hence, this research problem puts more emphasis on the challenges faced by the cloud based small IT firms and the way of developing a framework that specifically overcomes these challenges while staying within budget constraints. The researcher considered how small IT firms are able to enhance their security posture with open-source tools-based framework and how to identify the most suitable open-source resources for their business by considering the type of the business.

1.3. Research Questions

Through this research, the researcher expects to seek possible solutions for the following research questions.

I. How should a small cloud-based IT firms be prepared and respond to cyber security threats to protect their businesses?

II. What type of cybersecurity framework can be put in place to assist small IT firms to address operational and resource-related issues while minimizing cyber threats including phishing, malware attacks, data breaches, and unauthorized access?

1.4. Research Objectives

Research objectives are categorized into main objectives and specific objectives. Main objectives are represented to identify broader context of this study and specific objectives represents the achievable and distinct objectives.

1.4.1. Main Objectives

Through this research, the researcher expects to achieve the following goals.

I. Explore and understand modern cyber security threats for a cloud-based small IT firm environment.

This objective was achieved using two ways.

a) Data gathered through a survey and
b) By referring to the research conducted for the specific area.

Using the data that have been collected, identifying the existing security posture of the cloud-based small-scale businesses and identify the challenges that they face when implementing the security controls. Especially, the existing access controlling methods, existing cryptographic controls, existing password security implementations, methods that are followed for improving the employee awareness, what and how do they address the security incidents, what approaches are followed by them for collecting the evidence (Digital forensics), etc.

II. Provide a clear insight into the cyber security posture of cloud-based small IT firms.

Purpose of this objective is to gain a comprehensive understanding of the overall security status and readiness of cloud-based small IT firms. This objective involves assessing the security controls implemented by these organizations to secure their cloud environment. It also includes identifying the potential risks that may exist in the cloud infrastructure and applications being used by the small IT firms. Eventually, the findings of this research provide valuable insights and recommendations to help small IT firms for protecting their data and infrastructure in the cloud.

III. Identify what cyber security factors need to be implemented for securing the overall cloud-based small IT firms.

The objective of this research is to identify the specific cybersecurity factors that are necessary to secure a cloud-based small IT firms' environment. This could involve an analysis of existing security frameworks, industry best practices, and regulatory requirements that are relevant to cloud-based small IT firms. It could also involve an examination of case studies and real-world examples of successful security implementations in similar environments.

IV. Design and develop a cyber security implementation framework for detecting and mitigating cyber security threats for cloud-based small IT firms.

The objective of this research is to design and develop a cybersecurity implementation framework that can be used by cloud-based small IT firms to secure their IT infrastructure and data. This framework could include technical guidance with the tools and techniques that can be used for continuously improving the security of cloud-based small IT firms continuously.

1.4.2. Specific Objectives

The following are the specific objectives for this study.

I. Analyze open-source tools for identifying its features, limitations, and applications in different environments.

Open-source tools are software programs that are available for free and have a public license, allowing users to modify and distribute the code. In the context of cybersecurity, open-source tools can be a valuable resource for small IT firms, as they provide access to powerful and effective security solutions without requiring a significant financial investment. The objective of this research is to review and analyze the various open-source tools that are available for cloud-based small IT

firms. This could involve an analysis of the capabilities, limitations, and security features of each tool, as well as an examination of the effectiveness of these tools in mitigating common cybersecurity threats.

II. Identifying the application of existing cyber security frameworks in different environments and analyzing how those should be used in the framework according to the business type.

In this research, the researcher researched and examined the various cybersecurity frameworks that have been developed and implemented by researchers, cloud and cyber security experts, and practitioners in the field of cybersecurity. This can involve reviewing research papers, journals, books and other relevant resources to gain an understanding of the various frameworks and methodologies that have been developed to address cybersecurity threats and risks. Based on the identified applications of each cyber security frameworks, the researcher analyzed how those can be applied to the suggested framework.

1.5. Thesis Outline

The primary objective of this study is to establish an open-source tool-based security framework by identifying cyber security challenges that are encountered by cloud-based small IT firms and methodically implementing open-source cyber security tools-based framework. The introduction section emphasizes the necessity of improving the security of cloud-based small IT firms due to the growing number of security threats. It highlights the significance of an open-source tool-based approach in strengthening security postures of these cloud-based small IT firms.

The literature review thoroughly evaluates at identifying the gaps among cyber security standards, cyber security frameworks previously suggested by researchers and how open-source tools can be used for implementing the security of an organization. By identifying the limitations of the existing approaches, this section explains why a systematic, tool-focused cybersecurity model framework is necessary for enhancing the cyber security posture of small IT firms.

The research concept and implementation procedure are described in depth in the Methodology. It explains the detailed information about the survey that is conducted for small IT firms to identify the cyber security challenges they encounter and implementation of the model framework. The model framework consists with two main components;

I. Open-source cybersecurity tool recommendation system for IT companies that handles healthcare businesses' systems and retail businesses' systems.
II. Open-source cyber security tool catalogue.

For implementing these two components and examine the compatibility of the open-source tools, those were analyzed in virtualized operating systems such as Kali Linux, CentOS stream and Windows server, and prepared a dataset based on the collected information. The way of implementing content-based machine learning technique, and the tool catalogue, are explained in the methodology section.

The results and discussion section explains the findings of the survey analysis, evaluation of the open-source cybersecurity tool recommendation system and the features, success and efficiency of the model framework. In order to conduct the evaluation process, how the feedbacks are collected and analyzed were well explained in this chapter.

The study contributions are summarized up in the chapter, Conclusion and further research areas, which also emphasizes the significance of open-source cyber security model framework in cybersecurity. It outlines the main conclusions reached through the research and the ways in which the suggested framework improves security posture of cloud-based small IT firms. This section also makes recommendations for future research areas, such as incorporating more security domains into the framework.

CHAPTER 2

LITERATURE REVIEW

2.1 Gaps Among the Existing Security Standards

To discourse the cyber security issues for cloud-based platforms, many frameworks were suggested by researchers. A few researchers considered about the gaps among existing security frameworks.

2.1.1 Disconnection between Conceptual Models and Real-World Applications

While a number of previous studies provide thorough frameworks for controlling cybersecurity in cloud computing, a significant gap still exists in the implementation of theoretical models into practical solutions. As an example, Najat Tissir *et al* [11] has suggested a model for measuring the maturity level of cloud-based security domains of the organization. The Authors have implemented their model based on a capability maturity model which was implemented for cyber cloud security [24] by Ngoc T. *et al.* The researchers have considered 12 domains for implementing the capability maturity model such as Security of Infrastructure and Facilities, Identities and access management, Governance, Risk and Compliance Management, Incident Response, Data and Information Protection, Human Resource Management, Cloud Application Security, Security Awareness and Training, Audit and Accountability, Interoperability and Portability, Virtualization and Isolation and Cloud Connection and Communication Security. Based on these domains, they have represented the gap among the existing standards [24] as shown in the Figure 2. Their methodology combines international standards like ISO 27001, ISO 27017, ISO 27032, and the NIST CSF into a single model. The suggested framework takes organizational maturity, policy implementation, and compliance metrics into account in addition to the technical aspects of cloud cybersecurity. By outlining the ways in which different global standards can be combined, the framework provides a basis for creating workable, standards-compliant cybersecurity solutions for cloud-based systems.

However, these models lack any technological translations or recommendations for useful tools and is only conceptually provided. The absence of implementation guidelines poses a challenge to adoption for small IT firms.

2.1.2 Inadequate Cybersecurity Frameworks Created for Small IT Firms

Carlo Di Giulio *et al* as well performed a comparative review on existing standards and the new frameworks that have been suggested by other researchers [17]. The researchers have considered the completeness and adequacy of ISO/IEC 27001, Cloud Computing Compliance Control Catalog (C5) and Federal Risk Authorization Management Program (FedRAMP).

ID	Domains/Models	CSA	CSCC	ENISA	IBM	CISCO	ISIMC	FedRAMP	PCIDSS	SANS	SSE-CMM	ES-CMM	RMM	ISO	NIST-CSF	Number
1	Infrastructure and facilities security (IF)	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	13
2	Identity and access management (IAM)	✓	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓	11
3	Governance, Risk, and Compliance (GRC)	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	11
4	Incident response (IR)	✓		✓			✓	✓	✓	✓		✓	✓		✓	9
5	Data and information protection (DIP)	✓	✓	✓	✓	✓			✓	✓					✓	8
6	Human resources management (HM)		✓	✓	✓	✓		✓				✓		✓		7
7	Application security (APP)	✓	✓	✓	✓	✓	✓				✓					7
8	Security awareness and training (AT)			✓			✓	✓			✓		✓		✓	6
9	Audit and accountability (AA)	✓					✓	✓			✓	✓				5
10	Interoperability and portability (IP)	✓		✓			✓									3
11	Virtualization and isolation (VI)	✓				✓	✓									3
12	Cloud connection and communication (CCC)		✓	✓	✓											3

Figure 2: Security domains in the existing security frameworks [24]

The findings show that SMEs often suffer from inadequate budgets, low awareness, lack of dedicated IT teams, and minimal management support for cybersecurity, which is exacerbated by the belief that cybersecurity is only necessary for larger enterprises with complex systems. While the paper effectively outlines the internal and external factors that affect cybersecurity decision-making in SMEs, according to their findings, each one of them has their own weaknesses such as missing controls, which could make the entire architecture vulnerable to threats.

Hence, for protecting the cloud-based small IT firms, these frameworks do not provide efficient controls [17]. Alladean Chidukwani *et al* conducted a survey for small IT

firms for identifying cyber security challenges, research focus and recommendations. As the scholars have indicated, the Australian Signals Directorate (ASD) Essential Eight, can be used for protecting the organizations from the threats and NIST CSF provides a comprehensive policy guideline for securing the IT infrastructure from detecting, preventing and responding to cyber threats [9]. NIST has considered the cost effectiveness, and the requirement of having expertise within the small-to-medium businesses and hence, a simpler version of NIST CSF called *NIST Interagency Report 7621 (NISTIR 7621)* was implemented. In order to improve the security in small IT firms, NIST interagency report can be used. ISO/IEC 27001, C5, FedRAMP and NIST CSF are considered as qualitative frameworks.

The majority of existing frameworks make assumptions about the level of infrastructure and organizational maturity that SMEs frequently lack. For example, the adoption of NIST or ISO standards necessitates not just policy frameworks but also continuous technical monitoring, evaluation, and reporting, all of which demand resources, expertise, and time. There is less likelihood of significant acceptance in these contexts unless a customized, phased strategy breaks these frameworks down into key elements that SMEs can really implement. Hence, a significant gap in the literature is, there are no lightweight, modular cybersecurity models that SMEs may gradually adopt, ideally supported by free or reasonably priced solutions.

2.2 Suggested Frameworks by Previous Researchers

Previous researchers have suggested different frameworks for protecting the cloud-based IT infrastructure from threats by considering different security controls.

2.2.1 Cloud Performance and Security Alignment based Cybersecurity Frameworks

Muhammad Imran Tariq *et al* [27] has proposed an agent-based threat management framework for cloud computing. In the context of cloud computing, independent agents are utilized to manage resources, share assets, and secure networks. Monitoring

the cloud services and authentication for the cloud infrastructure can be done using these agents. According to the researcher, software and intelligent agents were not use to address the security issues in cloud previously. As a useful tool for evaluating the effectiveness of the information security system, they employed information security metrics methodologies to construct the IS Framework and present software agents.

As shown in Figure 3, the researchers have implemented an information security framework with six layers, using software and intelligent agent problem-solving techniques by considering threat assessments, threat mitigation tools, threat evaluation and, security policies and procedures [27]. An agent is a self-contained creature that can work constantly in a given environment on behalf of its host to complete a specific goal or set of tasks. Also, it does not require the assistance of its creator / host during the task completion process. In Cloud Computing, autonomous agents are utilized for resource sharing, troubleshooting and composition, and authentication. The use of agents in cloud computing is a new method to increase security, privacy, management of resources and storage, service discovery, processing management, and vendor negotiation [27].

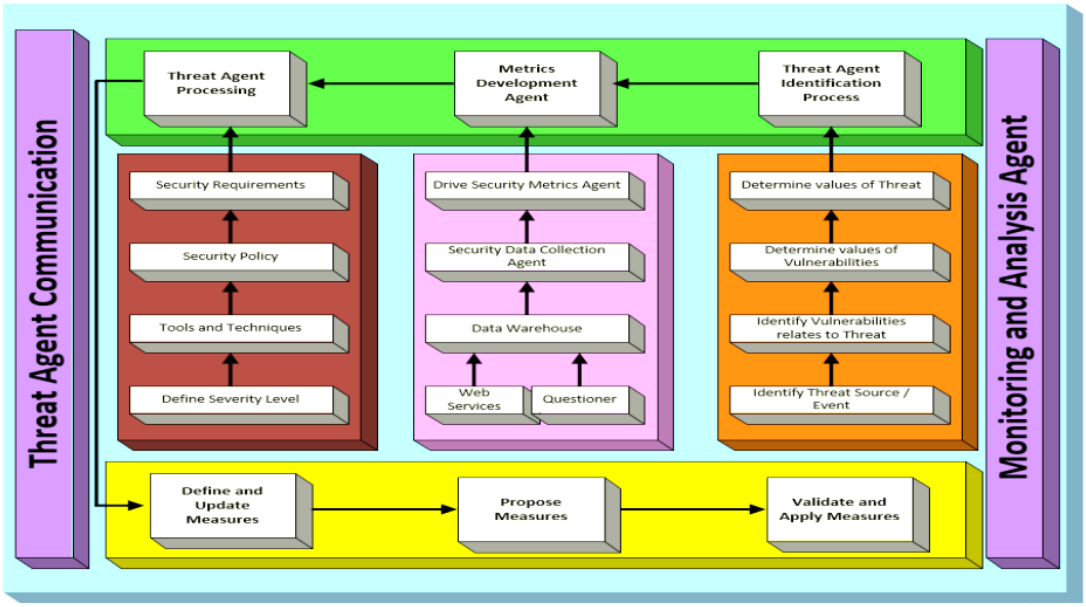


Figure 3: Agent based cyber security framework for cloud environment [27]

For managing the cloud security, a conceptual framework was suggested [11] as shown in the Figure 4. Prior to classifying the defined security practices or activities, they first describe the security practices and activities, aims and objectives, and security

needs. As the 2nd step, they decide on the metrics strategy and the technique to measure. In the 3rd step, a mathematical model was used for measuring the security metrics. As the next step, they analyzed the output of 3rd step, In the 5th step, maturity levels were identified and finally, security status and the impact to the management were considered.

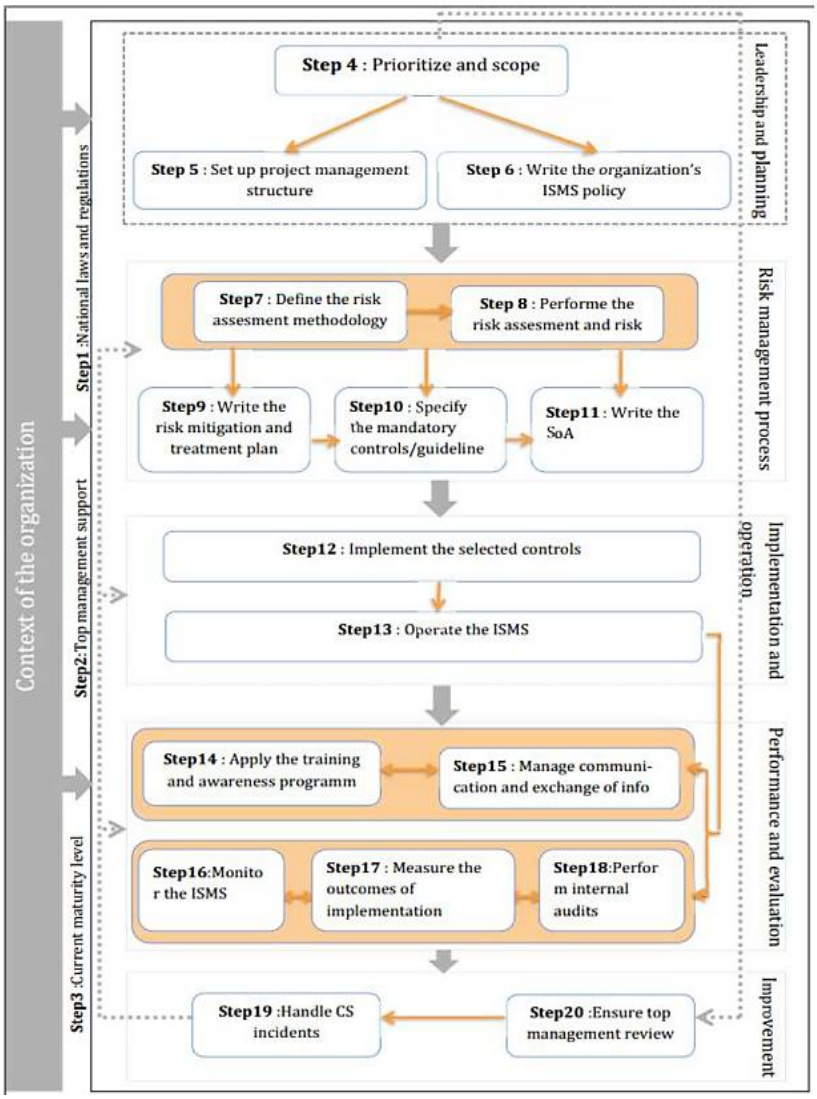


Figure 4: A conceptual Framework for Managing the Cloud Security [11]

Akashdeep Bhardwaj *et al* [7] have researched and implemented a four layered qualitative framework for improving the cloud performance along with cyber security. Four layers are;

- Define Taxonomy: Identify exactly what has to be measured.
- Define Metrics: Metrics for cyber security and cloud performance are defined in this layer and used for management level security requests.
- Quantitative and Objective Measurements: Master Service Agreements are considered in this layer.
- Reference Architecture: This specifies the procedures and guidelines put in place to adhere to the cyber security and cloud performance delivery

Their research highlighted the need for a metrics-based method to assess security and performance in cloud computing environments. The suggested approach emphasizes the necessity of methodically established metrics that may evaluate the effectiveness of service delivery while upholding robust security measures. The authors provided examples of real-time system behavior assessments using monitoring systems developed on open platforms such as Hadoop and OpenStack.
The implemented work is a technology independent framework and it indicates that the connection between the security and could performance be a positive relationship.
The cyber kill chain is another widely used framework, which focuses more on the technological aspect of Cyber Security [20]. Nevertheless, it did not adequately consider the human aspects of cyber threats like human error and insider threats. In Lee [20] has suggested a framework which focuses on cyber risk quantification along with the cyber ecosystem, for risk management and investment cost analysis. Suggested framework includes four layers as shown in Figure 5.

To accomplish holistic cyber risk management, all four layers are closely related to one another and to the framework for managing cyber risks.

2.2.2 Cybersecurity Frameworks Designed for Small IT Firms

According to Alladean Chidukwani *et al* [9], a limited number of researches have been done for the practical implementation of cyber security. They have suggested implementing more quantitative approaches since the qualitative approaches have been done deeper [9][20]. Hence it is important to implement a quantitative framework

that could use by the small IT firms. The NIST Cybersecurity Framework (CSF) played a crucial part in their thorough study, which concentrated on the cybersecurity requirements of small IT firms. The survey found that the majority of current cybersecurity implementation initiatives among SMBs focus mostly on the NIST CSFs "Identify" and "Protect" functions, paying little attention to the "Detect," "Respond," and "Recover" components.

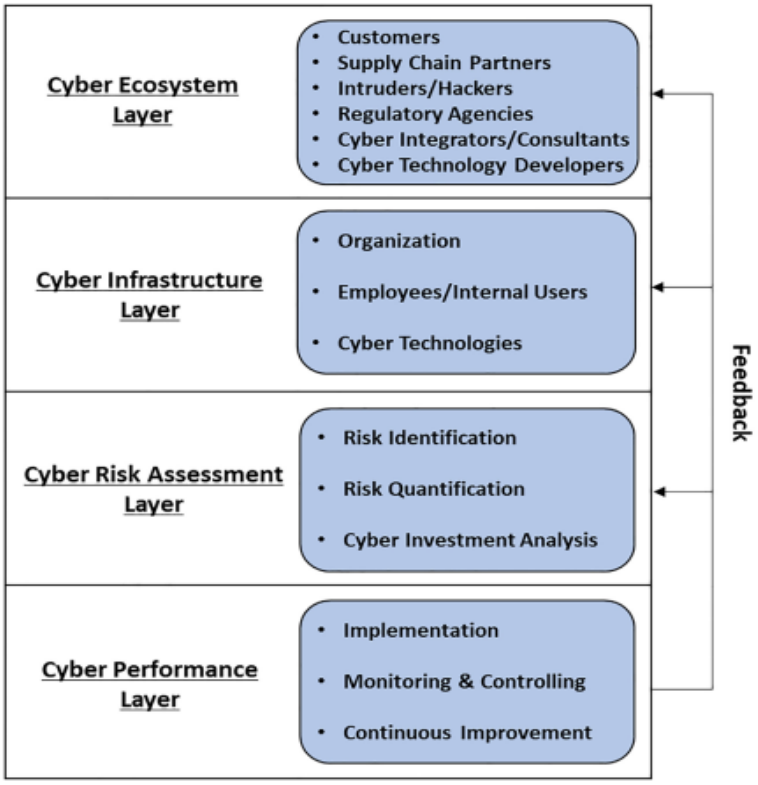


Figure 5: Risk Management and Investment Cost Analysis Framework [20]

As a core framework, the authors suggested a wider implementation of the whole NIST CSF. They also promoted hybrid systems that incorporate additional standards like as ISO 27001, PCI DSS, and ASD Essential Eight. Their research indicates that adapting the NIST framework to SMB use cases may improve security results, especially if combined with open-source, simpler implementations.

Hence it is important to implement a quantitative framework that could use by the small IT firms. Barry Sheehan *et al* [28] proposed a quantitative framework for risk

classification and assessment. In their work, the authors have a systematic way to rank the organizations based on their cyber security posture. As an overall of this research work, it combines with the bow-tie model for assessing the risks for the organization.

Landon McLilly *et al* [29] has proposed a cost-effective cyber security service solution that could be advantageous for cloud-based small IT firms. According to Figure 6, CODCSSSB is "*cloud-based on-demand cybersecurity service solution for small IT firms*" [29]. They have categorized cyber security service requests into five categories such as network security, application security, critical infrastructure security, cloud security and internet of things (IOT) security.

The researchers have explored the way of applying quantitative examination approach for assessing the service security requests to identify the weaknesses of the design or design issues with significantly lower cost.

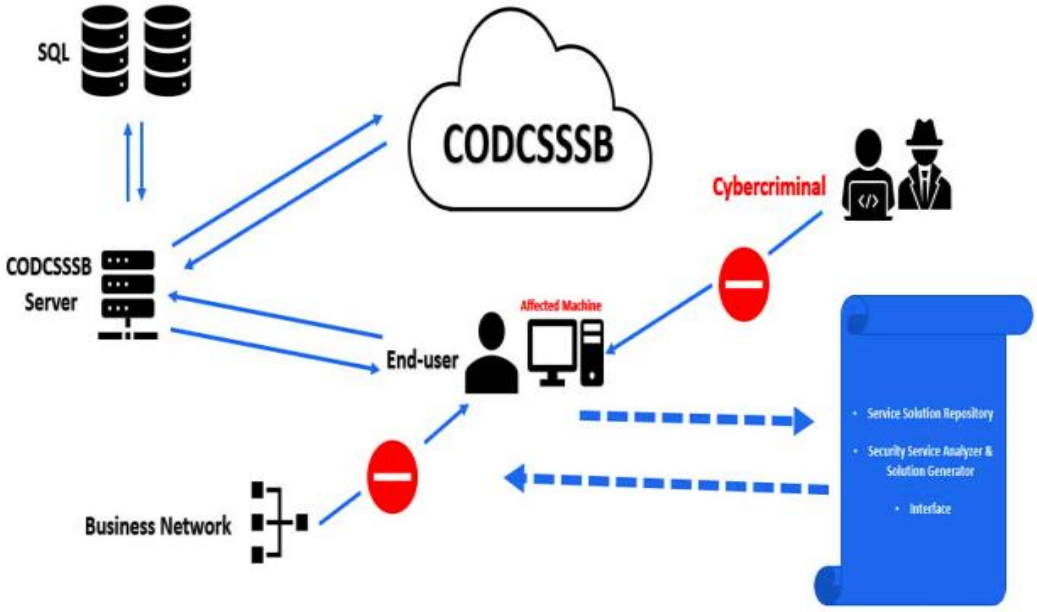


Figure 6: CODCSSSB [29]

A quantitative study was conducted by Frank Appunn *et al* [30], for defining efficient strategies to manage cyber security and IT governance for the leaders of small IT firms. Keke Gai *et al* [32] have suggested a method which is intended for matching different cyber risk situations that uses repository data. The suggested framework is maximizing the security level of an organization even under the financial issues and it has four

layers such as incident identification, cyber incident prevention, financial restriction response and recover management. This study is also proposing a conceptual method for reducing Cyber Insurance through this framework.

2.2.3 Cybersecurity Framework for Cloud-based Systems

Abdelrafe Elzamly *et al* [34] discussed and implemented a conceptual framework for banking organizations to cloud computing risk management. They have focused on privacy issues, legal issues, compliance and regulatory issues and security issues that are faced by banking organizations. In order to detect and evaluate cloud-specific risks including data leakage, service outages, illegal access, and compliance infractions, the framework presents a multi-dimensional modeling method. Risk identification, risk analysis, impact assessment, control selection, and ongoing monitoring are some of its essential elements. The researchers placed a high priority on risk prioritization using both quantitative scoring techniques and qualitative expert review, making ensured that limited security resources are allocated to the most important locations.

Adaptability and scalability are two of this framework's key advantages; it is platform-agnostic and appropriate for integration into cloud-hosted systems, independent of the underlying infrastructure. Furthermore, the framework offers actionable insights that may help decision-makers with budget allocation, vendor selection, and compliance alignment with standards like Basel II/III, GDPR, and ISO/IEC 27001 by mapping cloud risk indicators to useful control suggestions. Overall, the work of Elzamly et al. establishes the foundation for the creation of cybersecurity risk management systems that are open-source, standards-based, and lightweight which are necessary for cloud computing security.

Sumitra Binu *et al* [33] have suggested a security framework for cloud-based SaaS enterprise -level organizations. Suggested framework addresses the cloud in Physical, Network, Data and Application levels. And components of this framework are represented as physical security management module, data storage security management module, access security management module, application software management module and communication management module as shown in Figure 7. This framework's focus on multi-tenancy security, a prevalent issue in software as a

service platform where several customers share the same physical infrastructure, is one of its most notable aspects. The framework reduces the possibility of data exposure via unsafe APIs or shared resources by clearly establishing data and access boundaries. This framework works well with open-source and modular architectures from an implementation perspective. Every module may be created separately or combined with pre-existing tools like Kubernetes and OpenStack or SaaS platforms like ERPNext and Odoo.

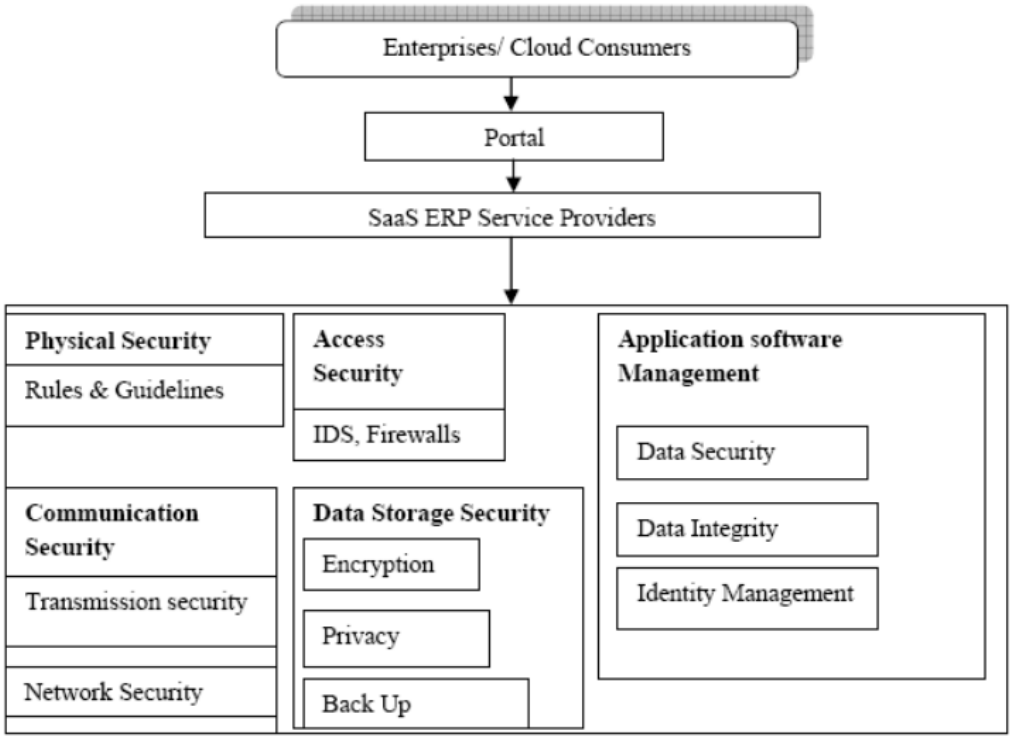


Figure 7: Cyber security framework for cloud-based enterprise level organizations [33]

The way of establishing the zero-trust strategy in cloud-based environment was discussed by Meheraj *et al* [36]. Their study has proven that the trust plays a crucial role in cloud security. According to the presented challenges, trust customization in cloud platforms, aggregation of trust information, evaluation of trust, trust assessment and qualitative and quantitative information derivation in the trust establishment process, were identified. The suggested model is implemented based on “never trust always verify” concept. Following the analyst's perspective, a trust model can improve

tracking and blocking of external attackers while limiting security vulnerabilities caused by insider attacks.

The proposed method can be used by the cloud service providers (CSP) to improve their security and their active involvement is necessary for implementation of the framework. Hence, this could be a disadvantage for the clients since they are required to wait until the necessary steps are taken by CSPs.

However, client-side security is also important for protecting the information from cyber threats. Ali Sakr *et al* [38] has suggested a client-side framework for protecting the privacy of health data that are stored in cloud. The researchers have indicated that the security that are provided by CSP are not sufficient. As an example, medical records may require higher level of security. The suggested method is to divide a given file into several parts and storing each part with a different cloud provider following encryption and permutation of the arrangement of the parts. The data required to decrypt and rearrange the file parts is kept in separate places on the client's premises. The suggested method allows the customer to take use of any security measures established by the cloud provider while still maintaining control over the security and privacy of their data.

A cloud computing adoption framework, which is a conceptual framework has been implemented by Victor Chang *et al* [39] and multi layered security mechanism is used to protect the business cloud. The suggested framework has developed and integrated firewall, encryption and identity management, and was able to successfully detect 99.95% malwares. Access Control and Firewall layer, focuses on password security, resource access control, and firewall protection. It ensures that only authorized persons have access to the network and protects against unauthorized network access. The second layer, known as the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), is in charge of detecting and blocking various forms of attacks, such as intrusion attempts and penetrations. Denial-of-Service (DoS), anti-spoofing, port scanning, known vulnerabilities, pattern-based attacks, parameter manipulation, cross-site scripting, SQL injection, and cookie poisoning are all prevented using advanced technology. Furthermore, it incorporates identity management procedures to ensure that only authorized individuals have access to sensitive information. The final layer, the Encryption/Decryption Control Layer is responsible for encrypting and decrypting

files, messages, and other data, as well as adding security measures. This layer not only monitors and alarms when certain entities exhibit anomalous behavior, but it also provides continuous assurance throughout the data transmission process. Following the detection of any anomalies, it comprises thorough investigation and remedy methods.

2.3 Open-Source Tools for Implementing Security

According to research, small IT firms may successfully handle real-world cybersecurity threats through the use of open-source software. Open-source technologies have been used by businesses with minimal resources to evaluate and strengthen their security posture, as evidenced by empirical case studies. In implementation, these technologies have been used to monitor systems, simulate attacks, find vulnerabilities, and strengthen defenses. Importantly, these results were obtained without the need for costly technical overhead or commercial licenses, demonstrating the feasibility of open-source implementation in environments with limited resources.

Furthermore, the academic works demonstrates that open-source solutions may handle the types of security operations that are usually considered to require enterprise-grade infrastructure. By using these open-source cyber security tools, small IT firms may independently and economically deploy meaningful security controls, challenging the false belief that only large organizations can afford robust cybersecurity.

2.3.1 The benefits of open source for SMEs in terms of strategy and operations

Ashok Yadav *et al* [41] have indicated that open-source tools (OSINT-Open-Source Intelligence) can be used to improve the security of organizations in various ways. It may strengthen cyber security by improving standard blacklists with context information and behavioral characteristics, allowing for more effective threat identification and phishing detection. In the opinion of the researchers, Open-source tools can be used for threat intelligence, keep the track of Advanced Persistent Threat (APT) activities, tracking malicious activities, digital forensics, HR recruitment and

many more. However, the researchers have emphasis that the need of using open-source tools in a legal and responsible manner. Open-source tools that are using for securing the IT Infrastructure, should not publish organization data into public. And tools should be adjustable for following data privacy and protection policies and during data collection, the authentication processes should not be broken. The researchers emphasize the need of creating a framework that includes all OSINT technologies and methodologies. As a result, the proposing framework in this research was based on open-source tools that can protect organizational information without releasing to the public.

2.3.2 Empirical Evidence for Real-World Application in SMEs

Real-world case studies are among the most persuasive ways to validate the usage of open-source software in small IT firms' cybersecurity. Berger, H. *et al* [43] have proved that open-source tools can be used to enhance the small IT firms' network security. Especially, open-source ethical hacking tools were considered.

The researchers examined into how a small IT firms utilizing free and open-source software that was able to establish a strong cybersecurity posture while having few financial and technical resources. This example demonstrates how open-source resources can fill the security gap that many small IT firms encounter since it is based on real requirement rather than theoretical design. The authors describe how the business used only open-source alternatives to conduct penetration testing, network scanning, and vulnerability identification even though it lacked an internal cybersecurity team or expert staff. More than 232 vulnerabilities were found and fixed as a result, indicating the tools' technical proficiency as well as their usefulness in enhancing the security posture of the business. Additionally, the report dispels the commonly held belief that only pricey proprietary solutions can provide adequate cybersecurity protection. It demonstrates that when open-source approaches are used, cost is not an impassable barrier to security. The case study also highlights how crucial accessibility and usability are to open-source development. In addition to being free, the tools used were user-friendly enough for people with no technical expertise to use. This highlights how open-source software has advanced to the point where it can be

deployed without the need for complex programming knowledge or network security experience, which makes it perfect for SMEs looking for quick and efficient security solutions.

2.3.3 Validating End-to-End Open-Source Integration with Conceptual Frameworks

A number of researchers have offered conceptual frameworks that incorporate open-source tools into more comprehensive cybersecurity designs built for business use, expanding beyond specific case studies. A conceptual model for improving the cloud security for DevSecOps have been implemented by Rakesh Kumar *et al* [42]. According to their research findings, cloud security can be improved performing;

- Continuous Security Monitoring: Tools for continuous security analysis of cloud environments can be provided through the open-source method. These technologies are capable of scanning for vulnerabilities, detecting malicious activity, and providing real-time alerts.
- For cloud-based application development, open-source technologies can enforce secure code principles. Developers can limit the chance of introducing vulnerabilities into their applications by following suggested secure coding techniques.
- Security Testing: Open-source tools can help with cloud application security testing. To discover and address security flaws, these technologies can automate security testing activities such as vulnerability scanning, penetration testing, and code analysis.
- Secure Containerization: Open-source tools can help with containerized application security. To ensure the security of containerized environments, these solutions can include container image scanning, runtime protection, and microservices firewall capabilities.
- Collaboration and Innovation: The open-source framework encourages developers and security professionals to collaborate and innovate. Organizations can benefit from the combined knowledge and skills of the

community by leveraging open-source software, leading to enhanced security practices and solutions.

- Flexibility and Agility: Open-source tools provide flexibility and agility in adapting to various cloud technologies and business scenarios. Organizations can select the best open-source technologies for their specific security needs, allowing them to achieve a balance of security, velocity, and agility.

2.4 Conclusive remarks

By referring previous researches, significant gaps among existing security standards, necessitating the development of new framework for cloud based small scaled IT firms were identified. Najat Tissir et al, and Carlo Di Giulio et al pointing out the necessity of efficient security controls for small scaled IT firms and suggested a model that offers a systematic way to assess the security of cloud-based organizations, emphasizing various domains like infrastructure, access management, and compliance. Numerous other researchers have various frameworks for addressing these missing security controls for small IT firms. The comparative analysis of standards conducted by Carlo di Giulio et al. showed flaws, emphasizing the need for more rigorous controls, notably for the protection of small IT firms.

Open-source tools have emerged as valuable assets for cybersecurity enhancement. They offer capabilities such as threat intelligence, secure code enforcement, access controls, etc.

By factoring in all of these, it is proven that open-source tools can be used to improve the security of IT infrastructure of a business without encountering significant difficulties. Hence, the demand for a technical-based and cost-effective framework for could-based small IT firms is necessary.

CHAPTER 3

FRAMEWORK AND RESEARCH METHODOLOGY

The research methods and techniques that was used in this research to implement a framework for improving the security posture of cloud-based small IT firms, are given in this section.

The Suggested methodology is given in the figure 8.

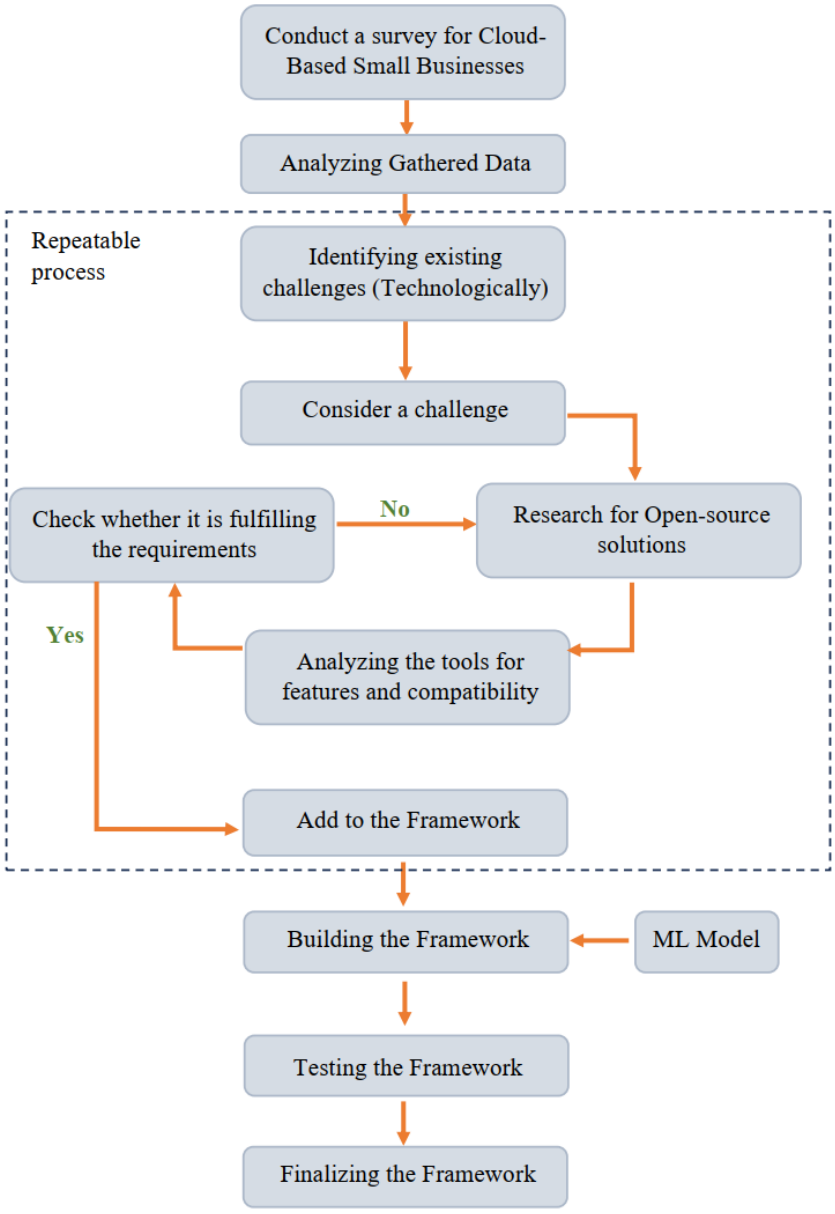


Figure 8: Research Methodology

3.1 Data Collection

Through a comprehensive survey, cyber security challenges for cloud based small IT firms were identified. According to the Organization for Economic Co-operation and Development-OECD, it is considered as small-to- medium business if the employee count is less than 250. The survey was created using Google form service and distributed among 70 small-to- medium businesses.

For this study, only two types of organizations were considered.

a) IT companies who are handling healthcare related businesses data.
b) IT companies who are handling retail businesses data.

Personally identifiable information (PII) of companies, were not gathered in order to prevent malicious activities on the companies that could be carried out using the information collected.

Questions of the survey was categorized into following sections.

Section 1: General Questions

Through the general questions, the researcher collected information regarding the working environment.

Question 01: Select your organization type
Answers (Options):

a) An IT company who is handling healthcare related businesses data.
b) An IT company who is handling retail businesses data.

Description: User was required to select their organization type from the given options.

Question 02: Do you have a dedicated IT security team or individual responsible for cyber security?
Answers (Options):

a) Yes, we do have a cyber security team
b) Yes, we have an individual who is responsible for cyber security
c) No, we do not have a cyber security team

Description: This question was asked to identify the current approach to cyber security within the small IT firms. Having a cyber security team or individual indicates that the cyber security is a consideration for enhancing the security posture of their company.

Question 03: Where are your products launched? (Depending on the country where you launch your products, security compliance regulations may vary)
Answers (Checkboxes):

a) Asia-Pacific
b) Europe
c) North America
d) South America
e) Africa
f) Middle East

Description: When a company launches a product, security compliance regulations can be changed according to the country/region and also the company may require to implement security controls within the organization to comply with certain compliance regulations. Hence, through this survey, the researcher collected information about the regions where products were launched.

Question 04: Do you have an internal network?
Answers (Options):

a) Yes
b) No

Description: Through this question, the researcher expected to identify if the company has an internal network. Having an internal network may require additional tools to secure the network and the end devices.

Question 05: Do you work remotely?

Answers (Options):

a) We are working remotely
b) We are following the hybrid method
c) We are working on site

Description: In order to identify the nature of the working environment, this question was asked. Users who work remotely vs users who works on site may have different requirements for tools. Hence, it is essential to identify the requirement and suggest the tools according to that.

Section 2: Policies and Procedures

Through the Survey, information about the existing policies and procedures of the organization, were collected. As the initial step of building security, it is essential to consider necessary security policies and procedures are in place. This information was used to identify lack of security controls defined and legal or regulatory requirements that the organization needs to be adhered to. The following set of questions were added to the survey for identifying the challenges in policy implementation and maintenance.

Question 06: Do you have any tool/service to create and maintain policies, guidelines and necessary agreement information for your organization?

Answers (Options):

a) Yes, we are using a premium tool
b) Yes, we are using an open-source tool
c) No, we are not using any tool

Description: Centralized policy and procedure management is necessary for small IT firms to standardization and ensuring consistency of the business by complying with necessary laws and regulations. In order to adhere to these laws and regulations, security controls such as versioning control, accountability, monitoring, etc. may be required. Tools can be used to easily maintain these documents and through this survey, the researcher collected the information about usage of tools for identifying the current procedure the small IT firms owners follow to maintain the policies and procedures.

Question 07: Do you have well-documented security policies in place?

Answers (Options):

a) Yes, we have implemented all the security policies and procedures
b) We have implemented a few policies, but some important policies are not implemented.
c) No, we do not have necessary policies in place

Description: Though this question, the researcher expected to identify what level of priority is given for the policies and procedure implementation and maintenance within the company.

Question 08: What difficulties do you find in managing/versioning the necessary policies, guidelines and agreements?

Answers (Checkboxes):

a) We do not have enough tools to build and track the changes made to policies, guideline and agreements
b) We do not have knowledgeable human resources to build the necessary policies, guideline and agreements
c) We do not have a centralized place to manage all the policies, guideline, agreements and their tracking information
d) We do not face difficulties and all the necessary policies, guidelines and agreements are implemented

Description: In order to identify the difficulties in managing policies and procedures, this question was added to the survey.

Question 09: How are these policies communicated to employees?

Answers (Options):

a) We share the policies through emails
b) We are using a premium tool for communicating the policies
c) We are using a open source tool for communicating the policies
d) We share the policies through our locally shared folder (through the internal network)

Description: It is essential to well communicate policies with the employees for better understanding of the security controls used within the organization.

Hence, this question was added to the survey for identifying what mechanisms are used by the companies to share the policies.

Question 10: What mechanisms are in place to ensure compliance?
Answers (Options):

a) We often conduct training sessions to ensure that employees understand the content of the policies
b) We conduct risk assessments to identify areas of non-compliance
c) We implemented necessary security controls to make sure that employees are unable to bypass the process flaw
d) We do not have mechanisms for ensuring the compliance

Description: For identifying what mechanisms are used to ensure the company is adhering to legal frameworks, regulatory requirements, industry standards and governance, this question was added to the survey. In order to avoid unnecessary legal disputes and fines, enhancing reputation and the trust of the company, standardizing internal processes, managing risks, improving safety of the working environment, etc., the compliance controls are required.

Section 3: Access Control and Authentication Mechanisms

Strong authentication and authorization systems are among the major pillars of access control. Authentication and authorization ensure that only people who are allowed can access sensitive information and resources. Through the survey, information about how access control is configured and managed within each organization were collected. Questions11-16 were added to the survey for collecting the information about current access control and authentication mechanisms.

Question 11: Do you use Multifactor authentication/ Biometrics mechanisms to login to your systems (cloud/ internal)?
Answers (Options):

a) Yes
b) No

Description: Multifactor authentication is a primary security control that can be used in many platforms and services. It is useful for reducing the risks related to the credentials and phishing while facilitating to meet regulatory requirements. Hence, this question was added to the survey for ascertaining whether respondents configure multifactor authentication or not.

Question 12: Are you using a secure VPN for accessing the resources/systems of the organization?

Answers (Options):

a) Yes, we are using a premium VPN solution
b) Yes, we are using an open-source VPN solution
c) No, we are not using any tool VPN solution

Description: In order to identify whether the responders are using a secure data transmission, this question was added to the survey. VPNs have the ability to encrypt data to prevent unauthorized access over the internet.

Question 13: How do you share passwords among office colleagues?

Answers (Checkboxes):

a) Chat Applications
b) Premium password sharing tool
c) Open-source password sharing tool
d) Emails
e) Printed/online sheets/documents
f) Phone Calls
g) Screen Sharing
h) We do not share passwords

Description: In order to identify whether the employees are following a secure password sharing method or potentially risky password sharing method, this question was added to the survey. For strengthening cyber security within a small IT firm, it is not recommended to share passwords through unsecure medias such as chat applications, emails, Printed/online sheets/documents, phone calls and screen sharing.

Question 14: Do you have any centralized tool (Access management system/ Ticketing system) to manage user access to cloud resources, including granting and revoking access?

Answers (Options):

a) Yes, we are using a premium tool
b) Yes, we are using an open-source tool
c) No, we are not using any tool

Description: Centralized access control facilitates the company to manage all the access controls in a one place and hence, the following can be achieved.

- Ability to enforce the access control policies within the company in an effective way.
- Systems can be easily audited and monitored for access control and hence, unwanted access controls can be revoked easily though simplified management of user roles and permissions.
- Sensitive information can be protected by having auditable and clear access control trails, while complying with the industry standards.
- With the growth of the company, managing access controls can be a challenge in a decentralized access control environment. Hence, using a centralized access control facilitates easy scalability.
- In order to response rapidly to a security incident, centralized access control may support for threat mitigation activities.

Question 15: Do you audit the access control lists for revoking unnecessary access privileges regularly?

Answers (Options):

a) Yes
b) Yes, But not regularly
c) No

Description: Revoking unnecessary access control is facilitates the company to prevent unauthorized access control and secure from the insider threats by reducing the attack surface. To ensure that, it is necessary to regular monitoring of access control. Hence, this question was added to the survey to assess the frequency of access control monitoring in small IT firms.

Question 16: What are the challenges you face when maintaining the access controls within your organization?

Answers (Lon answer text)

Description: This question was added to the survey for collecting the information about access control challenges which is not mentioned in this survey.

Section 4: Cryptographic controls

Cryptographic controls implemented within the working environment to protect the sensitive information of the organization was collected through the survey. Small IT firms can use a variety of cryptographic controls to prevent unnecessary accesses, unnecessary modifications, or information disclosures. The type of the control varies depending on the demands of the business and the types of information being handled. A Few examples for cryptographic controls as follow.

Use of Encryption: Encryption is the process of convert something readable (Plain Text) into an unreadable (Cypher Text) format using an encryption key and an encryption algorithm. The cypher text can only be read by the authorized parties who have the encryption keys. Encryption can be used to protect the data both in transit and rest. Hence, the file transferring, databases, storage devices, backups, etc. were checked for the encryption.

Use of Digital Signatures: Authentication and non-repudiation to electronic documents, messages, and transactions are provided by the digital signatures. Small IT firms can use these digital signatures for verifying the documents such as contracts, Agreements, orders, invoices are not altered.

Use of Hashing: When a message or file is hashed, a fixed-size digital fingerprint that is unreadable, is produced. Small IT firms can use

hashing to verify the accuracy of the data because any changes to the original message or file would result in a different hash value. Message authentication, file verification, and password storage are a few applications for hashing.

To obtain the information about cryptographic controls implemented, questions 17-19 were added to the survey.

Question 17: When you share confidential documents within the organization, do you encrypt the files?
Answers (Options):

a) Yes
b) No

Description: When sharing confidential documents within the organization without applying security controls such as encryption, those can be threatened with unauthorized accesses and modifications, Man-in-the-Middle (MitM) Attacks, insider threats, etc. Hence, this question was added to the survey to identify whether the responders are using file encryption before sharing the documents.

Question 18: How do you share confidential files with your office colleagues?
Answers (Checkboxes):

a) Emails
b) Chat Apps
c) We are using a premium tool
d) We are using an open-source tool
e) Google sharing option (For Google docs/sheets, etc.)
f) Other: _____

Description: In order to identifying insecure file sharing processes in a small IT firm, this question was added to the survey. When sharing confidential files with other colleagues, several methods such as emails, chat apps, google sharing method, etc. can be used. Among the given methods, using a premium tool or using an open-source tool can be considered as safest methods due to the following reasons to avoid other methods.

Emails: Using emails are easy to manage but can be easily attacked by phishing attacks. Another issue is human errors such as sending the emails to the wrong recipient may include confidential documents.

Chat Applications: Chats can be seen by anyone if they have access to the device. As an example, if an employee login to the same chat app through different devices (Ex. Mobile, Personal Laptop, Tab, etc.) and one device is compromised, all the chat history and shared confidential documents can be accessed by an unauthorized party.

Google Sharing Method: When compare with the emails and chat applications, google sharing method is having a few security controls implemented such as controlling access, disable download, edit options, etc. However, this method requires regular monitoring of the access given to the documents one by one and only has limited audit capabilities.

Question 19: Are you having offsite backups of your resources? How are they managed?

Answers (Options):

a) Yes, we have offsite backups and we encrypt those
b) Yes, we have offsite backups and we do not encrypt those
c) No, we do not have offsite backups

Description:

Data stored in the cloud can be threaten by insider attacks or ransomware. Hence, having offsite backups is a better way to continue their operations without any interruption. This question was added to the survey for identifying how responders are handling their offsite backups.

Section 5: Password Security

Small IT firms can use different password security tools to keep unwanted users out of their systems and sensitive data. The following information was gathered.

Password Managers: Users can create and store strong, individual passwords for various accounts using password managers. Password managers can be used in small IT firms to reduce the danger of password reuse.

Strong Passwords: Password rules that applied for employees, applications, systems, etc. were checked through questions 20 and 21 of this survey.

Question 20: Do you use a secure password sharing/storing tool for sharing/storing the passwords of systems owned by your organization?
Answers (Options):

a) Yes, we use a premium secure password sharing/storing tool
b) Yes, we use an open-source secure password sharing/storing tool
c) No, we do not use a secure password sharing/storing tool

Description: Using a secure password sharing/storing tool can be considered as the safest option for password sharing. Hence, this question was added to the survey to identify the current practice of password sharing.

Question 21: Do you enforce password security for the end devices?
Answers (Options):

a) Yes, we enforce password security
b) No, we do not enforce password security

Description: Weak passwords increase the risk of data theft, unauthorized access to company systems, and data breaches by giving cyber criminals access to end devices via cyber-attacks such as brute force, dictionary attacks, credential stuffing, etc. Through this question, the researcher expected to identify responders' current practice for end device security.

Section 6: Employee Awareness Trainings

To improve employee awareness, what methods are in place within the organization, how often the training programs are conducted, etc. information were collected with questions 22 and 23 of the survey.

Question 22: Do you provide your employees awareness training sessions on cyber security?

Answers (Options):

a) Yes
b) No

Description: If employees are not aware about security controls, they may engage in malicious actions that lead to a data breach unintentionally. Hence, this question was added to the survey to identify whether the responders conduct awareness sessions for their employees to enhance the security awareness.

Question 23: Do you have a dedicated tool for administering user awareness training, conducting simulated phishing tests, and similar activities?

Answers (Options):

a) Yes, we are using a premium tool
b) Yes, we are using an open-source tool
c) No, we are not using any tool

Description: In order to enhance the user awareness, planned simulated attacks can be conducted on the employees. Those kinds of attacks can be sent through security awareness training platforms. Hence, this question was added to the survey for collecting the availability information of tools that used for security awareness training.

Section 7: Incident Response

When a security incident occurs, it is required to have a proper incident response plan which guides how to respond to the incident. Through the survey, information about effectiveness of the incident response plan were collected. Questions from 24 to 26 were used to collected the information about current status of incident response methodologies that are used by the small IT firms.

Question 24: Are you using any tool/service for detecting and responding to security incidents?

Answers (Options):

a) Yes, we are using a premium tool
b) Yes, we are using an open-source tool
c) No, we are not using any tool.

Description: A violation of confidentiality, integrity and availability of data or any information system is called a security incident. These security incidents are caused intentionally by hackers or unintentionally by authorized users. Without having tools for detecting such incidents, those may remain unnoticed. Hence, this question was added to the survey for identifying the practices used for managing security incidents within the company.

Question 25: Is there a process in place for reporting security incidents?
Answers (Options):

a) Yes, we have implemented necessary processes, and users are well aware of those processes.
b) Yes, we have implemented necessary processes, but users are not aware about those processes.
c) No, we have not implemented those processes.

Description: With a well-defined process, employees of the company can rapidly inform about the security incidents to the necessary parties for taking immediate actions. Employees need to be aware of suspicious activities and have a solid understanding of the procedures in place in order to report them. Hence, this question was added to the survey to understand about security measures that are taken for reporting security incidents.

Question 26: How quickly are security incidents identified and resolved?
Answers (Options):

a) As soon as the incident is occurred and we will resolve it as soon as possible based on the criticality of the issue
b) We take some time to identify security incidents, and we will resolve them afterward.
c) Security incidents exist unnoticed because we do not have a proper tool to monitor them.

Description: In order to measure the effective of the incident response process, the following two measures are used.

- Mean time to detect (MTTD): Time duration of detecting the incident once it occurs. Fast detection may help to reduce the impact that occurred because of the incident on systems and data of the organization.
- Mean time to respond (MTTR): Time taken to respond to the incident. Faster successful responds to the security incidents may help to continue the business operations without any disruption.

Hence, this question was added to the survey for identifying efficiency on the incident detection and response process.

Section 8: Security Assessments and Auditing

The information about existing security assessments and auditing mechanisms that followed by the small IT firms, were collected though the survey. Information about risk assessments, vulnerability assessments, penetration testing, employee auditing, etc. was collected using the questions from 27 to 29.

Question 27: What challenges do you face when conducting security assessments and audits?

Answers (Checkboxes):

a) We do not have security expertise
b) We do not have enough tools (Open source / premium)
c) Complexity of technology
d) Higher cost of security
e) Other: _____

Description: Conducting security assessments and audits may be difficult for small IT firms due to higher cost of security, lack of security expertise and lack of resources. But still, security assessments and audits should be done for identify security related issues that related to the products and environment and complying with standards. Hence, this question was added to the survey for

identifying the challenges faced by small IT firms when conducting security assessments and audits.

Question 28: If you are using a third-party security service for security assessments and audits, do you sign the necessary agreements (Non-Disclosure Agreements - NDA, Service Level Agreements - SLA, etc.) with the service provider?

Answers (Options):

a) Yes
b) No

Description: Getting a service from third party security services is one option for small IT firms to improve their security. It is essential to have necessary agreements such as NDA, SLA, etc. in place for identifying the scope, roles and responsibilities and legal requirements that applies for third party service before receiving their services. To identify whether the company has necessary security related agreements in place, this question was added to the survey.

Question 29: Please list down other challenges you face when conducting security assessments and audits.

Answers (Long answer text)

Description: In order to find out what impediments small IT firms encounter when performing security audits and assessments, this question was added to the survey.

Section 9: Digital Forensics

Digital Forensic analysis can produce evidence for court cases or legal inquiries concerning cloud-based small IT firms. Many small IT firms must comply with rules and standards that are specific to their industry, such HIPAA or PCI DSS. To guarantee that cloud-based systems and services adhere to these compliance standards and prevent any penalties and legal liabilities, digital forensics can be used. Hence, through the survey, digital forensics tools and techniques were reviewed.

Question 30: Do you use digital forensics tools to conduct digital forensic investigations after an incident occurred in your organization?
Answers (Options):

a) Yes, we are using premium tools
b) Yes, we are using open-source tools
c) No, we are not using any tool
d) Yes, we are using both premium tools and open-source tools

Description: After a security incident is occurred, it is essential to investigate about the incident and find evidences and perform root cause analysis in order to prevent similar incidents from happening in the future. The purpose of this survey question is to find out what kind of tools small IT firms owners use for digital forensics.

Question 31: Is there a designated team or process in place for conducting digital forensic investigations in the event of a security incident?
Answers (Options):

a) Yes, we have both a designated team and processes in place
b) We have processes in place but no designated team for digital forensics
c) No, we do not have both a designated team and processes in place

Description: In the event of a security incident, having a specialized digital forensic team with established procedures may benefit in prompt recovery. Hence, this question was added to the survey for collecting the information about digital forensic practices that are used in small IT firms.

Question 32: Please mention other security challenges you face as a cloud-based small IT firm when implementing security in your organization.
Answers (Long answer text):
Description: In order to identify other security challenges that are not mentioned in this survey, this question was added.

3.2 Implementation of the Model Framework

The model framework is used to suggest the most suitable open-source cyber security tools for the users based on their requirements. Hence, the framework consists with two main components.

I. An open-source cyber security tools recommendation system: With the numerous open-source cyber security tools available in the cyber security ecosystem, small IT firm operators face difficulties in finding the most suitable open-source solutions for their operating environments. Hence, open-source cyber security tools recommendation system helps to identify the relevant and user friendly open-source solutions based on their requirements.

   In order to implement the recommendation system, two types of recommendation techniques were considered.

   a. Content-based Filtering Method

      In this filtering method, characteristics of the tools and users' preference are used to recommend the most suitable tools. Recommendations are made by finding the similar tools that align with the user requirements. This method is less computationally expensive and works well with personalized recommendations.

   b. Collaborative Filtering Method.

      Rather than considering the features of the tool, this method analyzes user interactions. As an example, users with similar requirements get similar tools each time. This method may require higher computational power to operate and able to provide diverse recommendations.

   Between these two methods, content-based filtering method was selected for implementing the recommendation system due to the following factors.

   a. Unlike collaborative filtering method, content-based filtering method recommends the tools based on the tools features and do not depend on the interactions of the users. In this study, tools features ser was the main resource that used.

   b. Cyber security professionals may have specific requirements about their operating environment. When that kind of situations are occurred,

recommendations can be customized to the user's interests using content-based filtering. In the collaborative filtering method, depending on the actions of other users, which might not always coincide.

c. In order to be effective, collaborative filtering method may require a large user base while content-based filtering method does not. Hence, it is easier to avoid cold start problem.

d. In collaborative filtering method, it has a greater likelihood to suggest the most popular open-source solutions most of the time because of user interactions analysis. Since the content-based filtering method is considering the tools features for the recommendations, it is possible to suggest highly relevant tools.

II. A tool information catalogue.

Community-driven and cost-effective open-source cyber security solutions can be used by organizations, developers, and security experts to create, test, and safeguard systems without being constrained by proprietary software. However, it can be difficult to choose the best open-source solution for a given use case due to the large number of open-source cyber security solutions accessible. Also, Information on these tools is frequently dispersed over several platforms, forums, and repositories since open-source development is decentralized. An open-source cyber security tools information catalogue is a useful reference in this situation and this issue is resolved through the collecting of data into a single, well-structured tool information catalog. This catalog offers comprehensive details on a wide range of open-source solutions under 12 domains as follows.

- Access Control: Unauthorized access can result in data leaks, financial loss, or service interruptions in a cloud environment where staff members, vendors, and remote workers regularly access company systems from various locations. Ensuring least privileges that given for the users are essential and can be achieved by access control tools.
- Ticketing Tools: For cloud-based small IT firms, ticketing tools are crucial because they offer organized security incident tracking, compliance enforcement, vulnerability monitoring, and access control management

thorough records of access requests, security incidents and logs. Hence, this category is grouped with the access control tools.

- Password Management: Since administrators and staff often use a variety of cloud services, apps, and platforms in a small IT firm that relies on the cloud, password security is a major concern. One of the main reasons for data breaches, account hacking, and illegal access is weak, repeated, or compromised passwords. By protecting, preserving, and automating password usage, password management tools assist reduces these threats and ensure a stronger cybersecurity posture.
- Policy Management: It can be difficult, time-consuming, and prone to errors to manually manage security policies across several cloud environments. In order to ensure that security and operational requirements are continuously followed, policy management solutions guide small IT firms in successfully defining, enforcing, and monitoring security policies. Centralizing security policies is one of the main purposes of policy management solutions, which facilitates the application and enforcement of regulations across all cloud services and platforms.
- Incident Response: Identify, address, and mitigate the cybersecurity threats in real time, incident response tools are essential for cloud-based small IT firms and using these tools helps to minimize the impact of security incidents and minimize downtimes. Hence, open-source incident response tools were considered for the catalogue.
- VPN Solutions: VPNs are providing secure and encrypted connection between the user and the cloud environment that accessed via public Wi-Fi or unsecured network. Without a VPN, small IT firms are more prone to cyberattacks, identity theft, and data interception, which makes it simpler for hackers to take advantage of cloud-based systems. Hence, VPN solutions were added to the catalogue.
- WAF Solutions: SQL injection, distributed denial-of-service (DDoS) attacks, and zero-day exploits and other cyber threats can be occurred at any time for these cloud-hosted applications. In order to defend cloud-based apps against these threats and ensure data security and business

continuity, a Secure Web Application Firewall (WAF) is necessary. Hence, WAF Solutions are considered for the catalogue.

- Phishing Simulation: Employees are frequently a small IT firms' first line of defense against online threats like phishing attempts in cloud-based businesses. Cybercriminals use phishing emails, texts, any other media that can be used to fool people into disclosing private information, such as user login credentials, bank or personal information. It is essential to increase the awareness about these attacks and conducting simulated attacks times to time for give them the real-world scenario experience. This may help users to identify and avoid real phishing attacks. In order to conduct these types of attacks, phishing simulated tools can be used and hence, those are included in the catalogue.
- Code Security Check-Git: IT related companies frequently use Git repositories such as GitHub, GitLab, or Bitbucket to store their IT projects and its data. An essential component of the development process are these repositories and if they are not well secured, they may also become a prime target for cyberattacks, particularly if the code has flaws, secrets, or configuration errors that an attacker could take advantage of. Hence, implementing code security is essential for securing their IT products. In order to protect CI/CD pipelines, identify vulnerabilities and prevent other code related weaknesses, these tools should be used.
- Anti-Malware: Cloud malware, which can propagate via compromised files, phishing emails, and unprotected endpoints, frequently targets cloud-based infrastructures. Anti-malware programs constantly check devices, apps, and cloud storage to find and remove malware before it can do any damage. Endpoint security and centralized monitoring are features of cloud-based anti-malware programs which assure the safety of any devices accessing cloud services.
- Awareness Implementing Platform: Maintaining regular security awareness training can be expensive and time-consuming for small cloud-based IT firms. Traditional security awareness programs frequently necessitate that companies pay instructors, hold personal sessions, and

repeatedly train new hires. Particularly for small IT firms with tight cybersecurity budgets, this can become an expensive burden. By offering automated, on-demand training, a Security Awareness Implementing Platform overcomes this issue and ensures that staff members obtain current security guidance without requiring ongoing manual training efforts.

- Security Assessment and Audit: In order to identify configuration errors, ensure compliance, and stop unauthorized access, security audits and assessments are crucial for small IT firms that use the cloud. Without involving a lot of manual work, these solutions assist companies in automating security monitoring, tracking system vulnerabilities, and generating compliance reports. Hence, security assessment and audit tools were considered for the catalogue.

This Catalogue acts as a thorough resource for users planning to explore and compare open-source solutions according to their features, compatibility, and practical uses. Finding new tools, and ensuring they choose the best solutions that satisfy their technical and business needs, can be achieve through this tool information catalogue.

The following steps were used to implement the model framework:

i. Analyzing tools for features and compatibility

ii. Dataset preparation: open-source tools

iii. Implementation of the machine learning technique for open-source cyber security tools recommendation system

iv. Implementation of the Tool Catalogue

3.2.1 Analyzing Tools for Features and Compatibility

After careful consideration of cyber security challenges that are faced by cloud based small IT firms which were identified through the survey results, open-source tools were analyzed to be used for overcoming those challenges. In order to ensure the

authenticity of the tool, the original website of the tool or official GitHub repository was used.

The ability of a software tool, application, or system to operate properly in a particular environment is known as compatibility. If these open-source cyber security tools are installing, running, and performing flawlessly without any issues or conflicts in different operating systems, it can be considered as the tool is compatible with the respective operating systems. Compatibility information is provided in the majority of these open-source tools' product documentations. However, the following factors led to the installation, configuration, and operation of the tools in a virtual environment for compatibility analysis.

- It is possible that vendors do not often update their documentation, particularly for older versions of Windows Server, Linux, or CentOS.
- Custom settings of the operational environment could affect the functionality of the tool or unexpected crashes.
- Yet, as the first step of the analysis, documentations were referred. Some of the open-source cyber security tools do not have a proper documentation implemented. Moving forward, the tools were installed and operated in the Linux, CentOS Stream and Windows server virtual machines. These operating systems are widely used operating systems [44] in many industries and hence, these operating systems were selected as the operating environments for analyzing the tools.

Virtual Machine environment was configured as follows.

- Used Virtualized Platform is VMWare Workstation pro and its network mode configured in to bridged mode. Hence, the VM is serve as a real network device.
- Used Virtual Machines are displayed in the table 1.

Table 1: Used Virtual Machine Information for Tool Analysis

VM	**Version**	**RAM**	**Disk Space**	**CPU**
Kali Linux	2024.2	8GB	100GB	4

CentOS Stream	9	8GB	100GB	4
Windows Server	2022	8GB	100GB	4

In order to verify the compatibility of the tool, the following steps were taken.

Step 1: Tool installation confirmation

After installing the tool in Linux, the tool installation success was verified using the following commands.

For Linux and CentOS Stream,

which <toolname>

or

dpkg -l | grep <toolname>

commands were used. For Windows server,

where <tool-name>

and

wmic product get name | findstr /I "<tool-name>

were used.

Step 2: Verifying that the tool starts up properly

Once the tool is installed successfully, it is verified that the tool is starting without any errors. In order to verify that, the following commands were used.

For Linux and CentOS Stream,

<toolname> --version

command was used.

For Windows server,

Event Viewer→ Windows Logs was used.

Step 3: Searching for errors in the logs

Log files offer up-to-date information on how an open-source cybersecurity tool interact with the system. The following commands were used for searching errors in the logs.

For Linux and CentOS Stream,

journalctl -u <service-name> --no-pager | tail -50 and *cat /var/log/<tool-name>.log*

commands were used.

For Windows server, Event Viewer→ Windows Logs was used.

Step 4: Cross platform testing

To compare behavior and determine whether any particular platform throws errors or has compatibility issues, tested the same security program on each virtual machine (VM) (Kali, CentOS Stream, Windows Server).

Overall, 97 open-source tools were analyzed under the following categories.

- Access Control and Ticketing: 25 tools
- Password Storing and Sharing: 6 tools
- Secure Document Sharing and Policy Management: 20 tools
- Incident Management: 8 tools
- VPN Solutions: 7 tools
- Web Application Firewalls (WAF): 8 tools
- Phishing Simulation: 3 tools
- Code Security Checking- Git: 3 tools
- Anti-Malware: 4 tools
- Security Awareness - Video quiz creation Platforms: 3 tools

- Security Assessments and Auditing Tools: 10 tools

The following details were collected about these tools.

- Link: Link to the online resource
- Documentation link: Link for the product documentation
- Suitability in healthcare products related businesses: In order to analyze this fact, data security controls, secure communication protocols, and security standards were examined. If the solution is having secure communication protocols, data security controls, it is considered as the tool is adhering to security standards such as HIPAA, GDPR, and SOC2. Hence, if the tool is adhering to all of these security controls, it was considered as a suitable tool for the healthcare product related businesses.
- Suitability in retail business products related businesses: This fact was analyzed by checking data security controls, secure communication protocols and security standards such as GDPR and SOC2. If the tool is adhering to these standards, it was considered as a suitable tool for the retail business products.
- Security of the open-source tool: The following details were collected by reading the documentation of the tools.
    - Secure Communication Protocols: In order to protect data confidentiality, integrity and availability, it is essential to implement secure communication in a application. For collecting this information, product documentation was referred and the following facts were considered.
        a. Secure API Communication: mutualTLS, JSON Web Tokens (JWT) and Hash-based Message Authentication Code (HMAC) were considered.
        b. Data-in-Transit Encryption: Whether the application facilitates to use TLS and HTTPS
    - Data Security controls: The selected data security controls were differ based on the type of the tool.

a. Access Control and Ticketing, Secure Document Sharing and Policy Management, Code Security Checking, Security Awareness - Video quiz creation Platforms: Session Management, Role Based Access Control (RBAC), Encrypted storage and Multi Factor Authentication (MFA) were considered.
b. Password Storing and Sharing: Secure password storage, end to end encryption (E2EE) and Secure key management were considered.
c. Incident Management, VPN Solutions, Web Application Firewalls (WAF), Phishing Simulation: Encrypted logs, TLS, HMAC, DDoS Protection and E2EE security controls were considered.
d. Anti-Malware: TLS and untampered logs were considered.

- Regular Software Updates and Patch Management

Based on the implementation of these security controls, security of the tool was considered.

- Community support: Whether the tool has active community for continuous implementation of the application and security, was examined. Open-source tools are required to have necessary bug fixes, security patches, and frequent updates for reducing the attack surface. Inadequate community support makes the tools unattended for security vulnerabilities. To confirm whether or not the tool has community support, the following steps were followed.
    - It is verified that the most recent versions of the tools and updated documentations are available to download in the official website.
    - If the tool downloading source is GitHub, the recent commits, pull requests, information about releases were checked
- Cost of the tools (free-1, costly-0): Some open-source tools has paid versions with better features while others have less features with the free version. Both

of these categories are considered for implementing the dataset. In order to find the pricing information, the tools' official websites were checked.

- User friendliness: Some open-source tools are only providing command line interfaces (CLI) while others are using graphical user interfaces (GUI) to work with the tool. When comparing with the CLIs, GUIs are easy to handle by non-technical users. Hence, for indicating the user friendliness of the tool, this factor was considered.
- Ability to fulfil the requirement: Different tools in the same tool category may have different features for performing the same operation. Some of the tools may not be able to fulfil the user requirements. Hence, the ability to fulfil the user requirement sufficiently with the tool, was considered.
- Compatibility with different OS: The users may require to install tools in different operating systems according to their existing working environments. Hence, the supported operating systems were considered for each tool.
- Direct Integration features with necessary services: Some users may require to integrate the open-source tools with their existing applications. The following are the few of widely used tools.
    - G-Suite
    - GitHub
    - Jira
    - Slack

  Hence, integration with these tools were considered. In order to check the integration capabilities, the official documentation was considered.
- Installation pre-requirements: In order to run an application without having any issues, it may require to meet some conditions or configurations before installing the tool. As a result of that Some additional services may require to be installed in the same working environment to function the application properly. Hence, those pre-requirements were considered.
- System requirements: Before installing the application, tools may require to have different hardware requirements or software requirements. The user needs

to have those requirements fulfilled initially and hence; system requirements were considered.

- End of Support: Whether the open-source product is actively updated or maintained by its community or contributors, was considered. When an open-source community or software manufacturer quits to provide updates, security updates, bug fixes, and formal support for a tool, it is known as End of Service (EOS). This situation makes the application vulnerable. Hence, whether the open-source product is actively updated or maintained by its community or contributors, was considered.

3.2.2 Dataset Preparation: Open-Source Tools

Dataset was made by the collected information after analyzing tools. The following are the features of the dataset.

- tool_category: tool_category feature indicates the category to which the tool belongs and was considered as a categorical variable.
- healthcare_business: This was considered as 1 if the tool is appropriate for handling data related to healthcare businesses.
- retail_business: This was considered as 1 if the tool is appropriate for handling data related to retail businesses.
- has_updates: If the tool receives updates recently and frequently, this was considered as 1.
- com_support: If the tool has an active community support, this feature was considered as 1.
- cost_free: Some of the open-source tools may costly solutions while others are free solutions. Hence, if the open-source tool is a free solution, it was considered as 1.
- useWith_Internal: Some of the small IT firms may have an internal network. For those kinds of businesses, some tools may not be used to fulfil their

requirement. Hence, if the tool can be used with the internal network, it was considered as 1.

- user_friendlyness: If the tool has a GUI, this feature was considered as 1.
- comp_linux: If the tool is compatible with Linux operating system, this feature was considered as 1.
- comp_windows: If the tool is compatible with Windows operating system, this feature was considered as 1.
- comp_centos: If the tool is compatible with CentOS operating system, this feature was considered as 1.
- inte_gsuite: If the tool can be integrated with GSuite, this feature was considered as 1.
- inte_github: If the tool can be integrated with Github, this feature was considered as 1.
- inte_jira: If the tool can be integrated with Jira, this feature was considered as 1.
- inte_slack: If the tool can be integrated with Slack, this feature was considered as 1.
- is_comply_hipaa: If the tool design is complied with HIPAA, this was considered as 1.
- is_comply_gdpr: If the tool design is complied with GDPR, this was considered as 1.
- is_comply_CyberEssentials: If the tool design is complied with Cyber Essentials requirements, this was considered as 1.
- is_comply_SOC2: If the tool design is complied with SOC2 requirements, this was considered as 1.
- selected_tool: Tool name

The dataset was created manually and a few factors make the dataset ideal for a content-based recommendation system. The dataset can be scalable and has rich metadata which assist in categorizing, organizing, and understanding contents of the

dataset. With these Instead of depending on user interactions, these dataset features allow for the computation of relevant tool recommendations. Additionally, the dataset covers a variety of categories, guaranteeing that suggestions are not unduly limited to a certain kind of too category.

3.2.3 Implementation of the Machine Learning Technique

In order to suggest the most suitable open-source tools set according to the user requirements, a content-based machine learning recommendation method was used. Content based recommendation method is a filtering mechanism that uses items' features to generate the recommendations for the users while compares with the user profiles which includes users' preferences. Hence, it can suggest similar items as user profile required. Figure 9 represents the implementation strategy of the filtering mechanism.

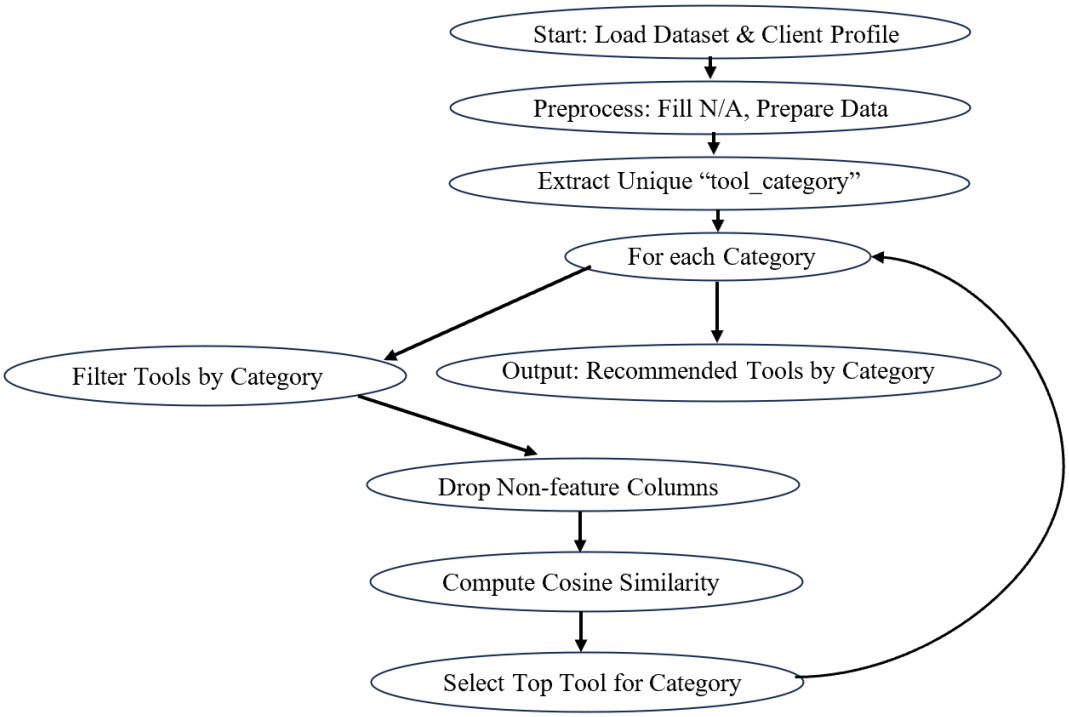


Figure 9: Implementation Strategy of the Filtering Mechanism

Step 1: Load the Dataset and Client Profile

The researcher collected the user requirements through the web application as shown in the figure 10. Client profile consists of environmental requirements that needs to be compared with the dataset. The following information are used for implementing the client profile.

Information about primary business area: In this question, users are asked to choose their organization type. Users are given the option to choose their company type because this study only looks at IT companies that manage healthcare and retail businesses.

Product Location details: The location information where the users' products were launched were collected. These information helps to identify what cyber security standards user should adhere to. Hence, the regions such as:

- Asia-Pacific
- Europe
- North America
- South America
- Africa

given for the users to select the relevant regions.

Internal Network information: Even if the users use cloud as their main resource for products, users might have an internal network within their organization which may include servers, databases, internal applications, etc., This on-premise infrastructure must be considered and well secured from cyber threats. In order to defend against endpoint security and network-based attacks, suitable open-source tools should be selected. Hence, this question was added to the user requirement gathering form.

As mentioned in the section 3.2.3, operating systems that are used in the working environment, vary from one organization to another. Hence, widely used operating systems were listed in this question for gathering the user requirements.

Users may need to integrate their systems with their existing applications such as G-Suite, GitHub, Jira or Slack.

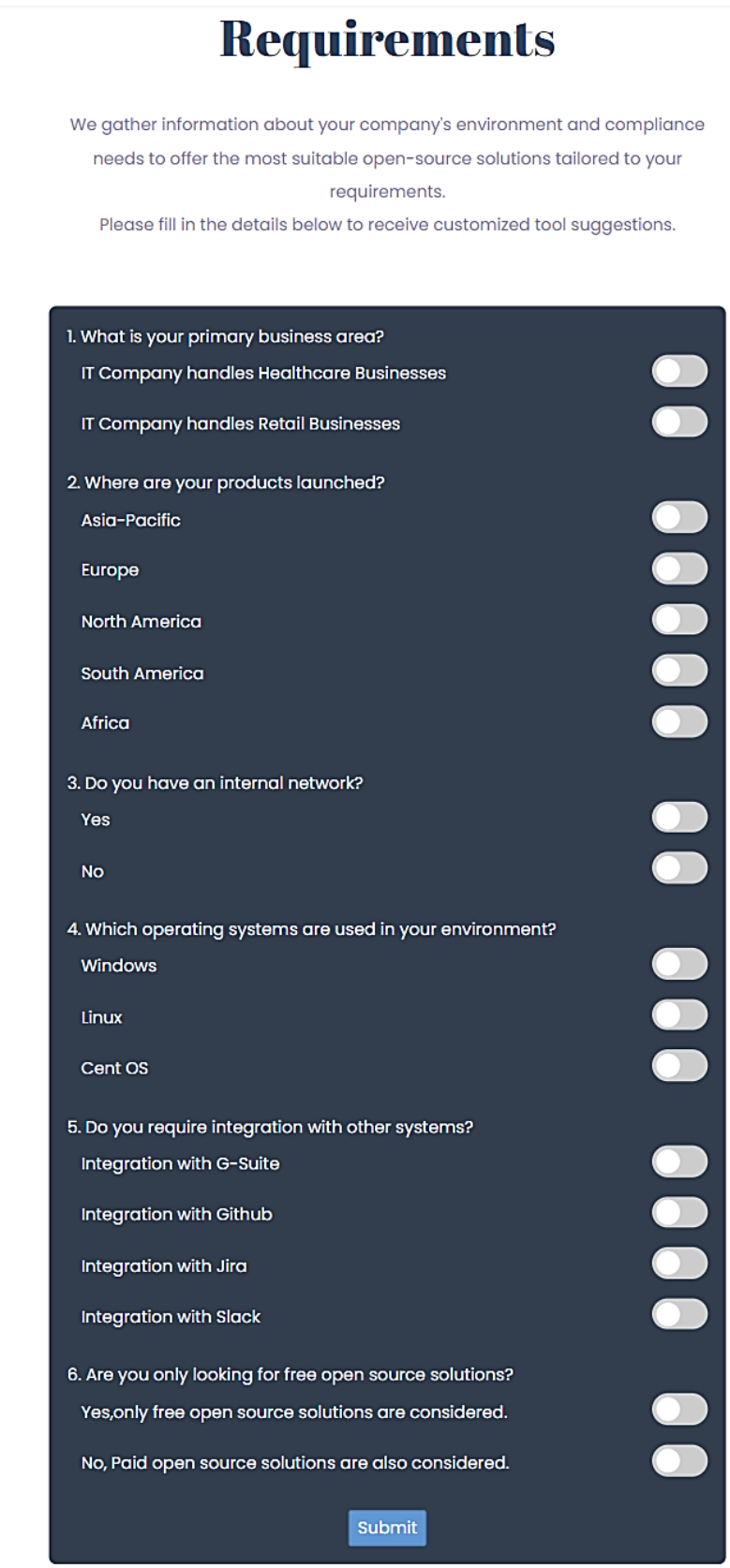


Figure 10: User Requirements Gathering Form

G-suite include applications such as Drive, Sheets, Google Docs, Google Forms, Google Calendar, Gmail, Google Sites, Google Meet, Contacts, Gmail business email and Google Workspace. These applications may include sensitive data and due to that reason, those must be protected. Code base of the most products that handled by cloud based small IT firms are launched in GitHub which may include credentials, source code and configurations of the projects. Therefore, GitHub should be protected from cyber threats. Jira or slack handles sensitive project related data which needs to be protected. Hence, this question was added to the user requirements form.

There are both free and premium versions of open-source tools. While some small IT firms have a minimal budget for implementing cyber security, the majority of small IT firms have a tight budget. In this study, we have considered both free and paid open-source tools and hence, with this question, colleting the user's expectation about the budget was collected. Sample client profile is shown in figure 11.

Step 2: Preprocessing the dataset

Data preprocessing is the process of getting all the collected raw data ready for analysis. In order to train accurate models, it is necessary to ensure that the data is consistent. Properly preparing the data improves model performance, resulting in faster convergence and higher accuracy. Preprocessing also improves data quality by making the dataset cleaner and more dependable. Finally, preprocessing increases the dataset's adaptability, making it suitable for a wide range of machine learning algorithms, ensuring the model can perform well across different approaches.

After collecting the user profile, that information sends to the content-based filtering system. Once both dataset and client profile are received, dataset is preprocessed. The data set includes missing values while duplicate values were not found. During the preprocessing, all the missing values was filled with 0.

Technologies Used: Pandas Data Frame, which is a python library used for data analysis and manipulation.

```
function getRecommendations() {
    // Collect user input data
    const data = {
        healthcare_data: document.getElementById('q1_healthcare').checked ? 1 : 0,
        retail_data: document.getElementById('q1_retail').checked ? 1 : 0,
        has_updates: 1,
        com_support: 1,
        only_opensource: document.getElementById('q6_Yes').checked ? 1 : 0,
        internal_network: document.getElementById('q3_yes').checked ? 1 : 0,
        user_friendlyness: 1,
        os_windows: document.getElementById('q4_windows').checked ? 1 : 0,
        os_linux: document.getElementById('q4_linux').checked ? 1 : 0,
        os_centos: document.getElementById('q4_centos').checked ? 1 : 0,
        intgrt_gsuite: document.getElementById('q5_gsuite').checked ? 1 : 0,
        intgrt_github: document.getElementById('q5_github').checked ? 1 : 0,
        intgrt_jira: document.getElementById('q5_jira').checked ? 1 : 0,
        intgrt_slack: document.getElementById('q5_slack').checked ? 1 : 0,
        regions: {
            apac: document.getElementById('q2_apac').checked ? 1 : 0,
            europe: document.getElementById('q2_europe').checked ? 1 : 0,
            na: document.getElementById('q2_na').checked ? 1 : 0,
            sa: document.getElementById('q2_sa').checked ? 1 : 0,
            africa: document.getElementById('q2_africa').checked ? 1 : 0
        }
    };
  const clientProfile = {
      healthcare_data: data.healthcare_data,
      retail_data: data.retail_data,
      has_updates: data.has_updates,
      com_support: data.com_support,
      only_opensource: data.only_opensource,
      internal_network: data.internal_network,
      user_friendlyness: data.user_friendlyness,
      os_windows: data.os_windows,
      os_linux: data.os_linux,
      os_centos: data.os_centos,
      intgrt_gsuite: data.intgrt_gsuite,
      intgrt_github: data.intgrt_github,
      intgrt_jira: data.intgrt_jira,
      intgrt_slack: data.intgrt_slack,
      ...compliance  // Spread compliance properties into the final profile
  };
```

Figure 11: Client Profile

Step 3: Extract Unique tool_category

The “tool_category” is a categorical feature and hence, it is used as a label to group tools.

Once this feature is used for labeling, it is no longer required for computing the cosine similarity. Hence, tool_category feature was dropped after grouping the tools.

Step 4: Filter Tools by Category

With the use of tool_category feature, each and every tool is identified according to their relevant category.

Step 5: Drop Non-feature Columns

If a dataset contains columns that are unrelated to the analysis or do not help the model make predictions, those were removed in this step.

Step 6: Compute Cosine Similarity

With the cosine similarity, it could be measured how similar the tool features compared to the client profile. Choosing Cosine Similarity is beneficial in a content-based tool recommendation system since it emphasizes the tools' inherent characteristics rather than depending on user interactions or preferences. This recommendation system makes advantage of item-specific characteristics such tool category and other features because it is not reliant on the user's prior behavior. Cosine similarity compares these vectors based on their direction (i.e., the similarity in characteristics) rather than their magnitude by representing each tool as a vector in a high-dimensional space.

This method works well when suggesting tools that have similar features but aren't connected to a specific user's previous interaction. When suggesting cybersecurity technologies, for an example, cosine similarity can be used to find tools that have comparable use cases or overlapping features, like access control tools, incident response tools, etc.

The following is an example on how it works.

Ex:

Question: What is your primary business area?

- User selects IT company handle healthcare businesses → assign 1

- User selects IT company handle retail businesses → assign 2

Where are your products launched?

- User selects Asia-Pacific → assign 1
- User selects Europe →assign 2
- User selects North America →assign 3
- User selects South America →assign 4
- User selects Africa →assign 5

After assigning values each and every client requirement and dataset features, it would be appeared as follows.

Client profile vector: [1,4,3,2,1,2]

Tool A vector: [1,3,3,1,0,1]

Cosine Similarity (Client Profile[A], Tool A [B]) = $\frac{A.B}{||A||\,||B||}$

Calculation of A.B: (1.1) +(4.3) +(3.3) +(2.1) +(1.0) +(2.1) =13.9

Calculation of Magnitude vector ||A||: $\sqrt{1^2 + 4^2 + 3^2 + 2^2 + 1^2 + 2^2} = \sqrt{35}$

Calculation of Magnitude vector ||B||: $\sqrt{1^2 + 3^2 + 3^2 + 1^2 + 0 + 1^2} = \sqrt{21}$

Cosine Similarity = $\frac{13.9}{\sqrt{35}\sqrt{21}} = 0.5127$

In order to find the most suitable tool, cosine similarity of each tool will be calculated.

Calculated cosine similarity for Tool A: 0.5127

Assume cosine similarity for Tool B: 0.9543

Assume cosine similarity for Tool C: 0.2436

Among Tool A, Tool B and Tool C, highest similarity will be considered as the most suitable tool. Hence here, the Tool B is considered as the recommended tool for the relevant category.

Correspondingly, tools were selected for each category.

3.2.4 Implementation of the Tool Catalogue

The model framework consists of a comprehensive guide and offer detailed information about open-source cyber security tools. Creating an organized framework to effectively store, manage, and retrieve cybersecurity tool information is necessary to implement a tool catalogue. The following are the displayed information in the framework.

- **Tool introduction and its features**: Users can use this part as a reference to easily understand the functionality, features, and technical details of a tool, allowing them to make well-informed choices according to their security demands. Updates to cybersecurity tools' functionality, integrations, and compliance could be changed often. Hence, the tool catalogue should keep up to date by generating the most recent information rather than depending on out-of-date descriptions. Latest contents about the tools are generated using Gemini AI 2.0 Flash API for the framework. Gemini AI provides a cost-effective solution for creating excellent tool descriptions without displaying the static content for the users.

  In order to get the response from Gemini AI API, the request prompt was sent similar to the following text.

  ”<tool_name> open source tool introduction and explain its features”

  The following is the sample output for tool name “Keycloak” from the Gemini AI API.

  “***Introduction***

  Keycloak is a free and open-source Identity and Access Management (IAM) solution. It's a comprehensive platform that handles authentication and

authorization for applications and services, providing a single place to manage users, roles, and permissions. Think of it as a central identity provider that simplifies the process of securing your applications and APIs.

Here's a breakdown of its key features:

Core Features:

a) *Authentication: Keycloak offers a variety of authentication methods, including:*

   - *Username/Password: Standard login using credentials.*
   - *Social Login: Integration with popular providers like Google, Facebook, Twitter, etc.*
   - *OAuth 2.0 and OpenID Connect (OIDC): Industry standard protocols for secure authorization and authentication, allowing applications to securely access user information without directly managing credentials.*
   - *SAML 2.0: Another widely used standard for exchanging authentication and authorization data between security domains.*
   - *Multi-Factor Authentication (MFA): Enhanced security by requiring multiple verification factors (e.g., OTP, hardware token).*
   - *Kerberos: Authentication protocol commonly used in enterprise environments.*

b) *Authorization: Keycloak enables fine-grained control over access to resources:*
   - *Role-Based Access Control (RBAC): Assign users to roles and grant permissions based on those roles.*

- *Policy-Based Authorization: Define complex authorization rules based on various attributes and conditions.*
- *Attribute-Based Access Control (ABAC): Authorization decisions based on attributes of the user, resource, and environment.*
- *User Management: Keycloak simplifies user administration:*
- *Centralized User Management: Manage users, groups, and roles from a single console.*
- *User Federation: Connect to existing user directories (LDAP, Active Directory, etc.).*
- *User Self-Service: Empower users to manage their own profiles and passwords.*
- *User Registration and Account Management: Provide users with a streamlined registration and account management experience.*

c) *Protocol Support: Keycloak supports a wide range of industry-standard protocols:*
   - *OAuth 2.0: For authorizing access to protected resources.*
   - *OpenID Connect (OIDC): For verifying user identity.*
   - *SAML 2.0: For single sign-on (SSO) across multiple applications.*
   - *REST API: For programmatic access and integration with other systems.*

Additional Features:

- *Administration Console: A user-friendly web interface for managing users, roles, realms, and other Keycloak configurations.*
- *Extensibility: Keycloak can be extended with custom themes, authentication flows, and other add-ons.*

- *Scalability and High Availability: Keycloak is designed to scale to handle large numbers of users and applications. It supports clustering for high availability.*
- *Auditing and Logging: Provides comprehensive auditing and logging capabilities for security and compliance.*
- *Client Management: Manage different applications (clients) that connect to Keycloak. Define their access permissions and configure their authentication flows.*

Keycloak vs. Other IAM Solutions:

While other IAM solutions exist (Okta, Auth0, Azure Active Directory, etc.), Keycloak stands out as a powerful, open-source alternative. This offers greater flexibility, customization, and control over your IAM infrastructure, although it may require more technical expertise to set up and manage than some commercial solutions.

In summary, Keycloak is a robust and versatile IAM solution suitable for a wide range of applications and use cases, from small projects to large enterprise deployments. Its open-source nature, comprehensive feature set, and support for industry-standard protocols make it a compelling choice for organizations seeking secure and scalable identity management."

- **Download and installation guide**: In this section, the framework provides the download and installation guide of the tool. If the original updated official tool document was available, it was directly added to the framework as shown in figure 12. A docker file/ link to an official docker file was provided to the user for easy installation.

  The download and installation guides were added to the tool catalogue due to the following reasons.

  Easy Access: The official download links and installation instructions are easily accessible to users without requiring them to search through

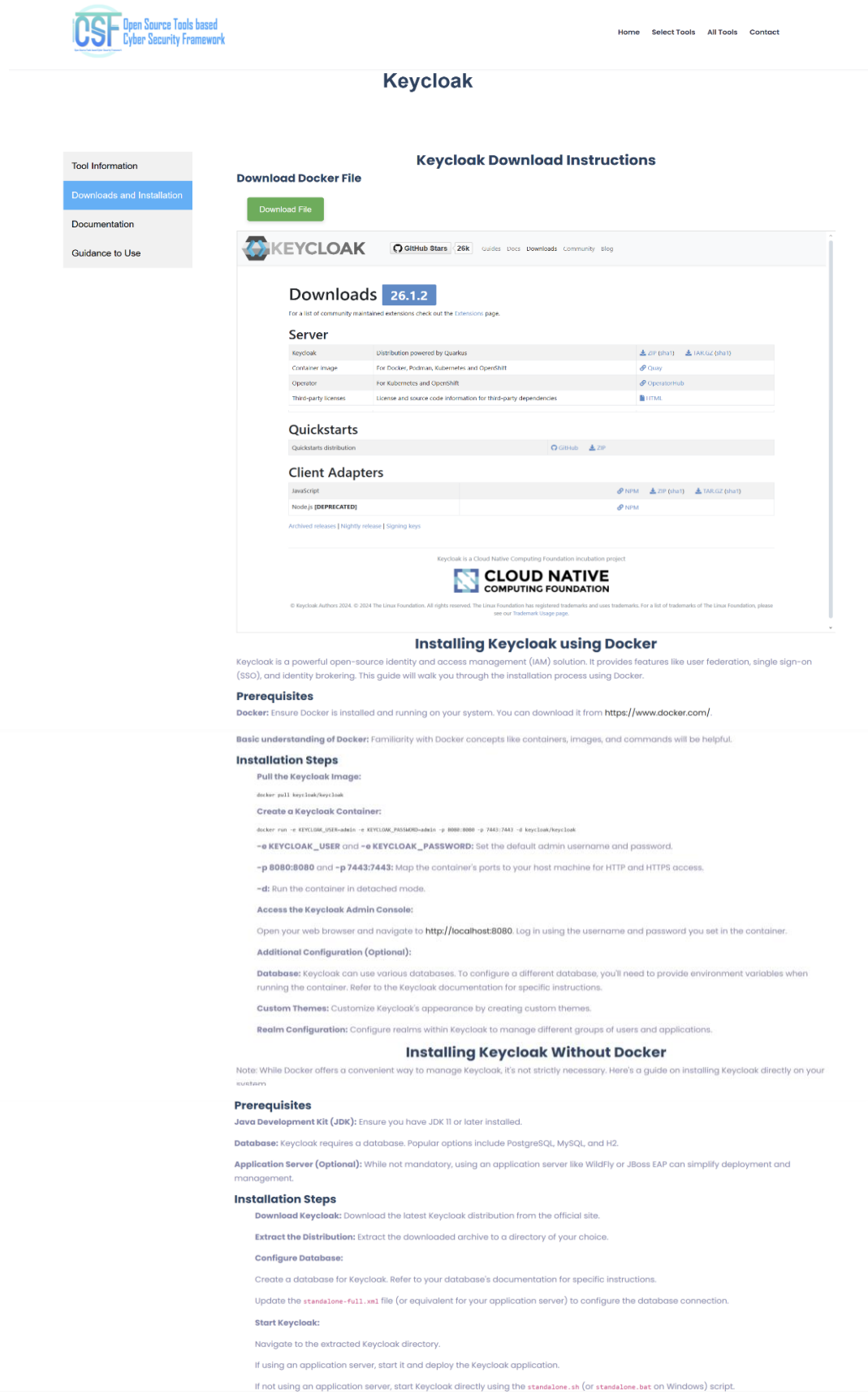


Figure 12: Download section on the Framework

numerous sites. They are less likely to download altered versions because they are guaranteed to get the tool from reliable and secure sources.

Minimizing configuration issues: A lot of security tools require particular configurations or dependencies. Giving users detailed instructions ensure they can install the tool correctly without having any errors.

- Tool documentation: Official tool documentation provided if the user requires further guidance. Same as the download section, the official documentation link or the documentation was directly added to the framework.
- Usage guidance: In this section, user is given a practical advice on how to use the tool effectively for securing their environments. The following are the reasons for adding the usage guidance for the tool catalogue.

  Not every tool on the list may be familiar to users. Clear instructions can assist users immediately grasp how to use the product, minimizing confusion and making the catalogue accessible.
  By following the correct guidelines and best practices, users may use the capabilities of the tools in the best way, completing jobs more quickly and with fewer mistakes.

3.2.5 Final Product

The final product is a web application and following are the technologies used to implement the application.

- Web Application: Basic programming languages like HTML, CSS and JavaScript were used for implementing the web application.
- Machine Learning Technique Implementations: In order to implement the recommendation system, pandas, scikit-learn (sklearn) libraries and Python 3 was used.

- Establish the Connection between web application and machine learning technique: Flask Framework, which has in build Development Server was used.

The figure 13 is representing the architecture of the product implemented.

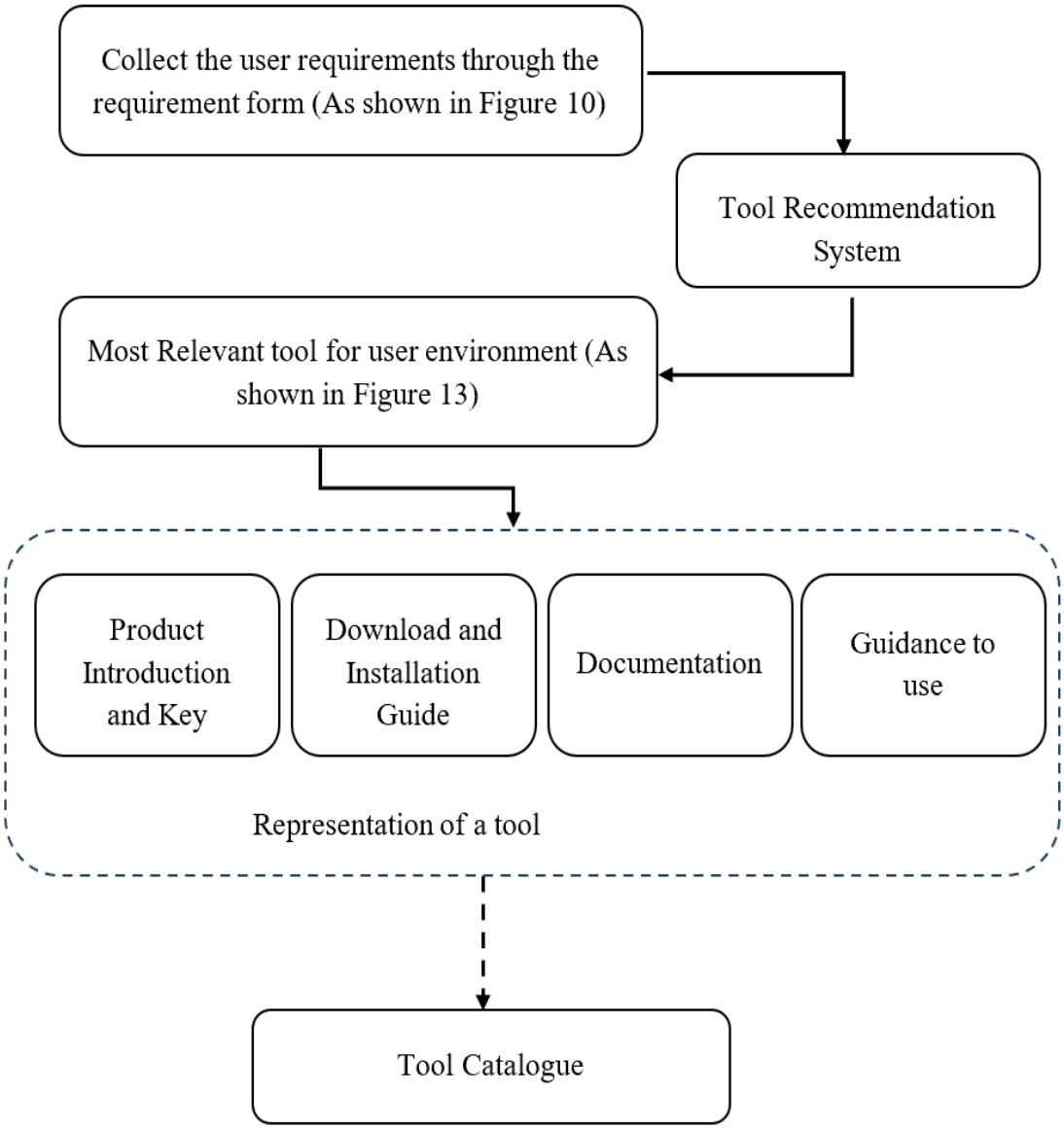


Figure 13: Product Architecture

As shown in figure 10, once the requirements are collected from the user, the suggested tools are displayed as shown in figure 14. Partial view of the implemented tool catalogue is shown in figure 15.

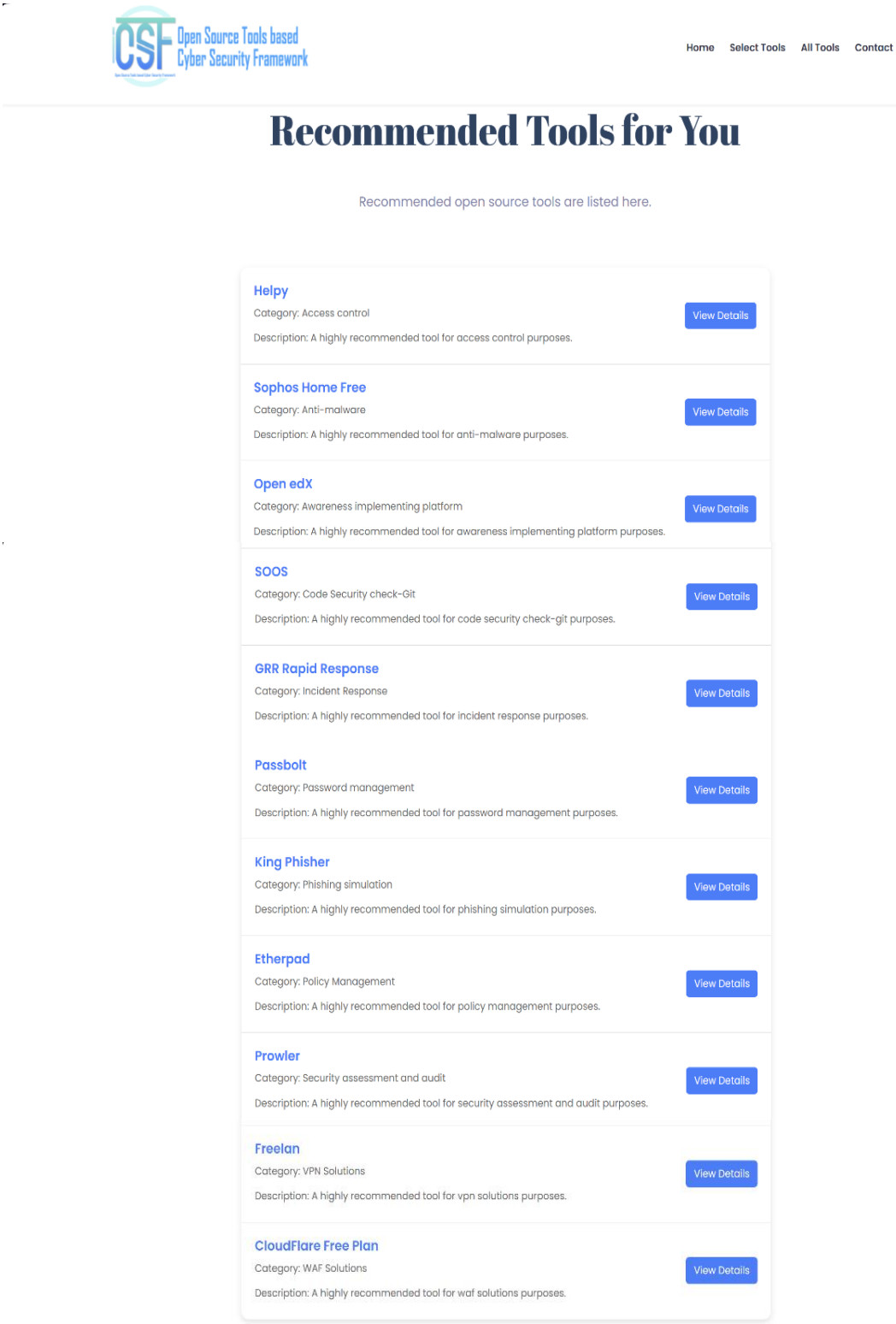


Figure 14: Suggested Tools List from the Recommendation System

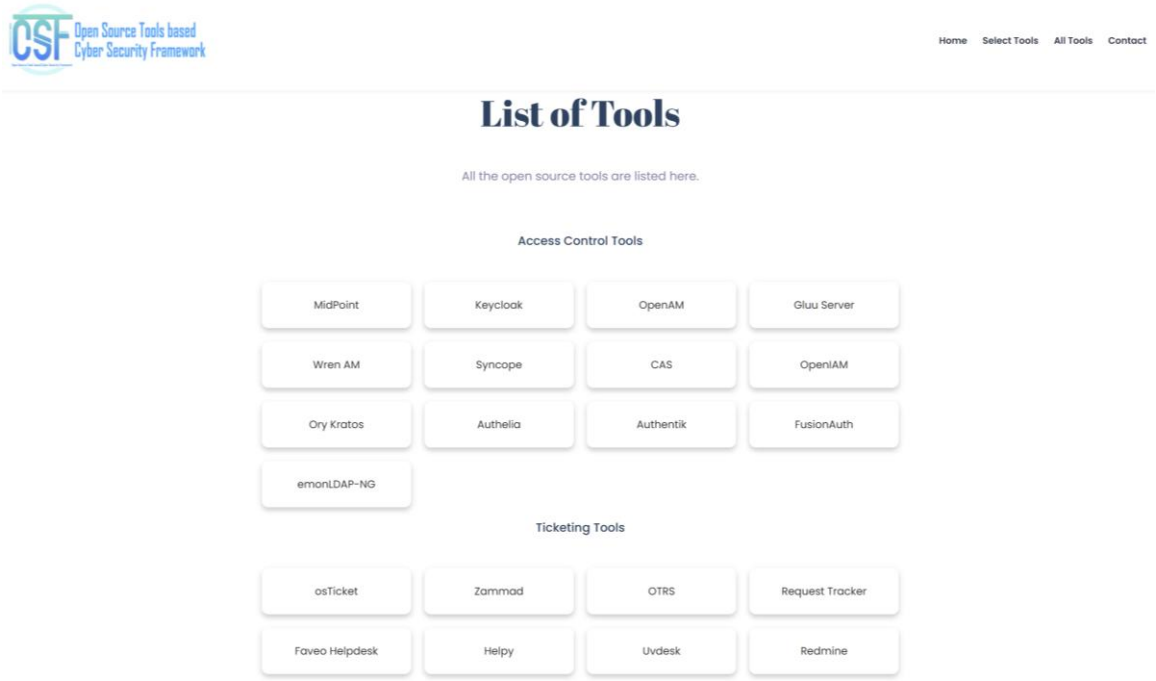


Figure 15: Tool Catalogue Preview

3.3 Chapter Summary

This chapter presented the methodological approach follows for the development of open-source tool based cyber security framework tailored for cloud based small IT firms. The chapter began with the survey conducted for determining challenges that cloud based small IT firms encountered. Once identifying the cyber security challenges, the framework established during this study is expected to be simple and flexible while addressing fundamental cybersecurity requirements such access control, VPNs, malware protection, incident response, etc. Features and the compatibility of the tools were considered in different environments and the dataset was created using the collected information. In order to suggest the most suitable tool from each category, a content-based filtering method, which was widely used in recommendation systems, was used. As a part of the same study, a tool catalogue was implemented with the guidance for users to download, install and use the tool. Documentation of the tool is also provided.

Additionally, case study evidence, conceptual models from previous research, and a study of strategic fit for SME environments was used as a guidance for the design.

CHAPTER 4

RESULTS AND DISCUSSION

In this chapter, we are presenting the data analysis in accordance with the primary research objectives that were established at the start of the study. To determine the main cybersecurity issues that cloud-based small IT firms encounter, a survey was carried out as part of this study. The purpose of the survey was to learn more about the effectiveness of current security measures, common security issues, and small IT firms owners' awareness of cybersecurity best practices. The analysis of survey data indicated several types of persistent issues, such as inadequate password management procedures, inadequate access control systems, a deficiency of effective incident response plans, budget constraints, and a lack of knowledge about cloud-compatible security products. Detailed analysis of the survey is presented in section 4.1. These results gave important background information for creating the cybersecurity tool catalog and recommendation system, significant knowledge into tool selection, compatibility, and user experience are provided by the deployment of the cybersecurity tool catalog and the tool recommendation system. Access control, incident management, anti-malware, password management, and web application firewalls are just a few of the many categories covered by the tool catalogue, which was created as a centralized source for open-source cybersecurity tools. Each tool in the catalogue has been organized based on its primary purpose, platform compatibility, and use cases in order to make it easy to follow.

The recommendation system was dependent on a number of factors, including the user's stated goals such as working with different operating environments, working for projects that are in different regions, integrating the security tools with their existing applications, etc. A weighted approach was used by the recommendation system to identify the most suitable tools according to these criteria. Kali Linux, CentOS Stream, and Windows Server 2022 were used in a virtual environment to conduct the compatibility analysis, which focused on open-source tools in the catalog. On every platform, the tools' performance, setup, and installation were examined. Though some needed certain configuration modifications to function properly.

Once implementing the proposed solution, it was sent to industry experts and collected the feedback about the suggested tool list for each category. The results were analyzed using precision at K method which is explained under section 4.2.

4.1 Analysis of Responses Collected Through the Survey

The survey was distributed to 70 small IT firms and only 31 of them responded. With a 44% response rate, insightful information from small IT firms were collected through the survey.

Among 31 organizations that responded to the survey, 18 of them are IT companies who handles retail businesses data and other 13 organizations handle healthcare related business data. 67.7% of small IT firms that responded to the survey do not have a cyber security team or an individual who is responsible for cyber security. The following are the challenges small IT firms face as derived using the survey results.

- 74.2% companies do not have necessary policies in place and most of them do not have enough tools to build and track the changes made to policies, guidelines and agreements in a centralized way. 80.6% of small IT firms are using emails for sharing these policy, guideline and agreement documents.
- 61.3% small IT firms do not have proper mechanisms for ensuring the compliance controls.
- 64.5% of small IT firms do not have centralized access control management and do not use multi factor authentication (MFA) and VPNs for secure accessing the internal systems. As the password sharing method, most of them are using chat applications and emails. Some of the small IT firms manage large spread sheets for maintaining the access control records, which is not very successful.
- 90.3% of responders are using emails to share confidential files while 71% of them are not encrypting those confidential files. 32.3% of responders are use chat applications as the media to share confidential files.
- 35.5% small IT firms do not maintain offsite backups while 29% of having backups but do not use security controls to protect those.

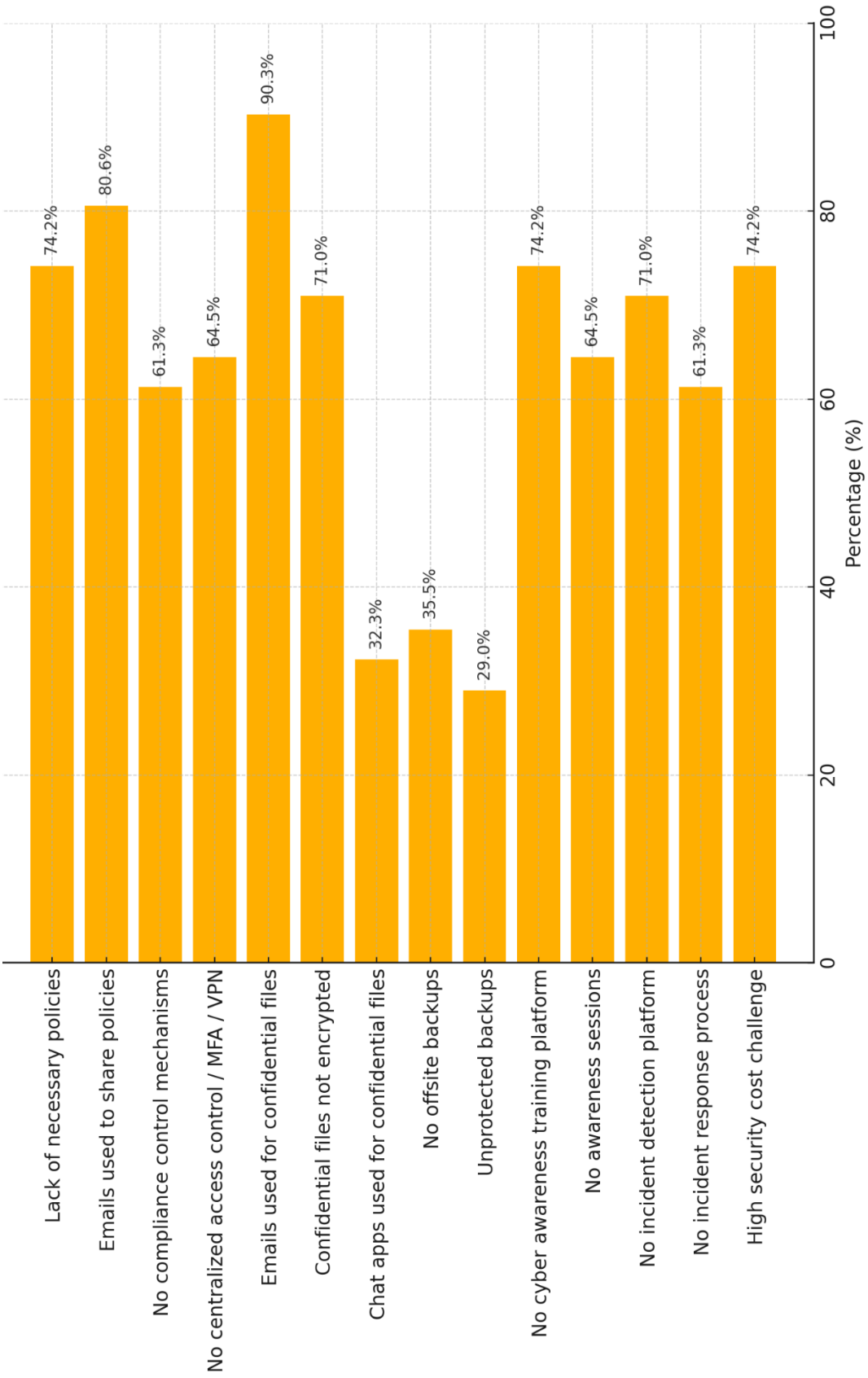


Figure 16: Cybersecurity Challenges in Small IT Firms

- 74.2% organizations do not use any cyber security awareness training platforms and 64.5% organizations do not conduct security awareness sessions for their employees.
- 71% of small IT firms do not have incident detecting and responding platforms and 61.3% of them do not have necessary processes defined for reporting security incidents. Hence, those security incidents remain unnoticed.
- When conducting security assessments and audits, 74.2% responders stated that higher cost of the security is one of the main challenges they face. Except this, lack of security tools and security expertise were stated as other challenges.

Figure 16 shows the challenges faced by small IT firms.

4.2 Evaluation of the recommendation system

After implanting the framework, it was required to collect Industry Experts' (IEs) opinion about the suggested tools based on their provided requirements. In order to collect the feedbacks, each industry expert provided 5 responses after checking 5 different environmental requirements. Users were given feedbacks with the feedback form that was implemented in the same web application as shown in the figure 17.

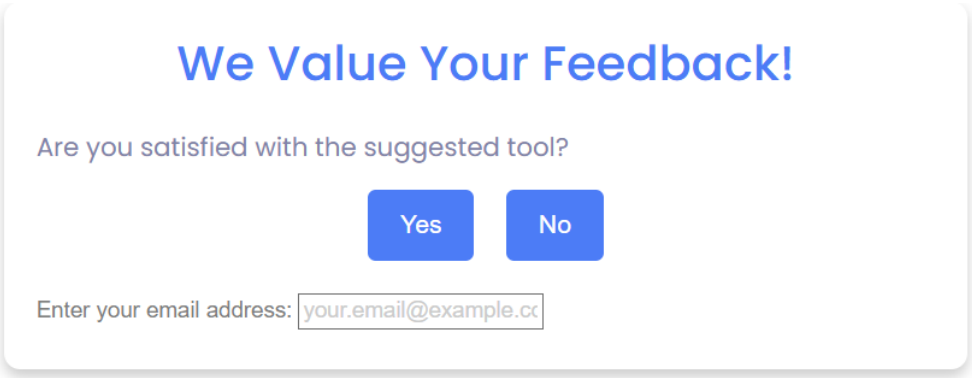


Figure 17: Feedback Form

If industry expert satisfies with the tools list that was recommended by the system, they are able to provide their confirmation with the "Yes" response. If they are not

satisfied with the tool suggestion, another web interface as shown in figure 18 will appear for providing the most suitable tools for according to their opinion.

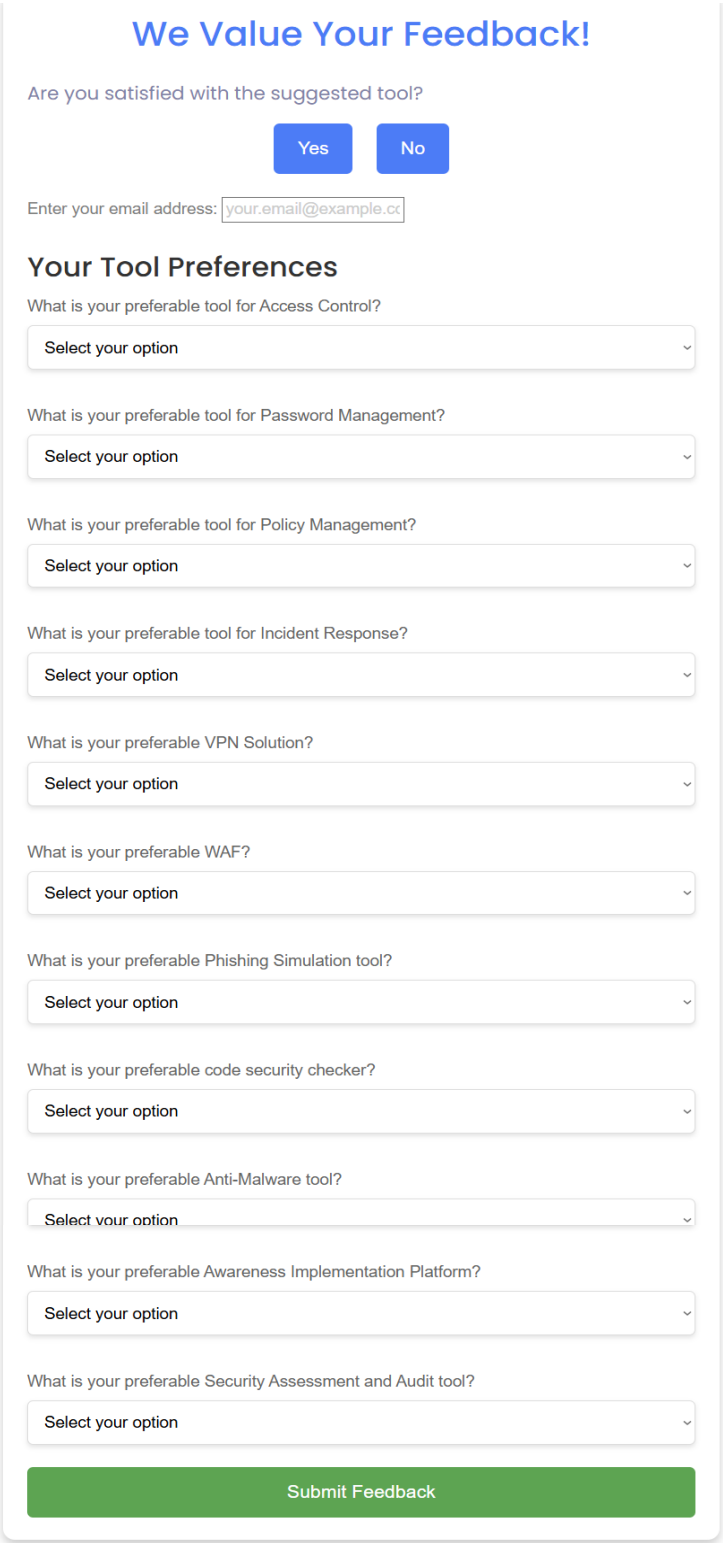


Figure 18: Feedback Form for Unsatisfied Responses

The evaluation results as follows.

There were 40 responses were collected from the industry experts and 87.5% of responses were agreed with the suggested open-source tools. For the rest, the industry experts suggested different tools according to their knowledge and experience.

In order to improve readability, instead of using full terms of the following requirements are shortened.

Table 2: Short Forms for Requirements

Question	**Answers (Full Term)**	**Answers (Shortened term)**
What is your primary business area?	IT Company handles Healthcare Businesses	Healthcare
	IT Company handles Retail Businesses	Retail
Where are your products launched?	Asia-Pacific	Asia-Pacific
	Europe	Europe
	North America	North America
	South America	South America
	Africa	Africa
Do you have an internal network?	Yes	Internal
	No	No Internal

Which operating systems are used in your environment?	Windows	Windows
	Linux	Linux
	Cent OS	Cent OS
Do you require integration with other systems?	Integration with G-Suite	G-Suite
	Integration with GitHub	GitHub
	Integration with Jira	Jira
	Integration with Slack	Slack
Are you only looking for free open-source solutions?	Yes, only free open-source solutions are considered.	Free Open Source
	No, paid open-source solutions are also considered.	Any Open Source

The following table 1 is representing the samples from collected responses that was given by one industry expert.

Table 3: Responses of the User 1

Environment Requirements	**Suggested Tools by the Recommendation System**	**Response**
Healthcare	Faveo Helpdesk (Access control)	Yes

Asia-Pacific Internal Linux GitHub Free Open Source	Sophos Home Free (Anti-malware) Open edX (Awareness implementing platform) SOOS (Code Security Check-Git) Cyphon (Incident Response) Passbolt (Password management) King Phisher (Phishing simulation) Paperless-ngx (Policy Management) OpenVAS (Security assessment and audit) Freelan (VPN Solutions) WebKnight (WAF Solutions)	
Retail Asia-Pacific, Europe No Internal Linux G-Suite, GitHub Free Open Source	Ory Hydra (Access control) Malwarebytes (Anti-malware) ILIAS (Awareness implementing platform) SOOS (Code Security check-Git) OSSIM (Incident Response) Bitwarden (Password management) King Phisher (Phishing simulation) Paperless-ngx (Policy Management) OpenVAS (Security assessment and audit_ OpenVPN (VPN Solutions) CloudFlare Free Plan (WAF Solutions)	Yes
Healthcare Europe Internal	Ory Hydra (Access control) Sophos Home Free (Anti-malware) Open edX (Awareness implementing platform)	No SAP-Credential Digger (Code

Centos Github Jira Free Open Source	SOOS (Code Security Check-GitHub) OSSEC (Incident Response) Passbolt (Password management) GoPhish (Phishing simulation) Cryptomator (Policy Management) Prowler (Security assessment and audit) OpenVPN (VPN Solutions) IronBee (WAF Solutions)	Security Check-Github) Malwarebytes (Anti-malware)

For recommendation systems, Precision at K method is a broadly applied method for the evaluation. Precision at K value is between 0 and 1 while the value is near to 1 considered as the relevant and values near to 0 is considered as Irrelevant. By using this method, accuracy level of the recommendation system can be measured.

$$p@k = \frac{Number\ of\ relevant\ items\ in\ the\ top\ K\ predictionser}{k}$$

$$p@k = \frac{Number\ of\ relevant\ tools\ (According\ to\ IE)}{Number\ of\ suggested\ tools}$$

Table 4: Precision at K Value for Collected Responses

	Response 1	Response 2	Response 3	Response 4	Response 5
IE 1	11/11 = 1	11/11 =1	11/11=1	11/11=1	9/11=0.818
IE2	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1
IE3	11/11 = 1	10/11=0.909	11/11 = 1	11/11 = 1	10/11=0.909
IE4	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1

IE5	11/11 = 1	10/11=0.909	11/11 = 1	11/11 = 1	11/11 = 1
IE6	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1
IE7	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1
IE8	11/11 = 1	11/11 = 1	11/11 = 1	11/11 = 1	10/11=0.909

Mean of p@k = (0.9636 +1 +0.9636 +1 +0.9818 +1 +1 +0.9818)/8

Mean of p@k = 0.98635

The value for Precision at K is 0.98635 and it is considered as a better performance.

Hence, this recommendation system was able to achieve 98% user satisfaction level.

4.3 Discussion

The results demonstrate how well the cybersecurity product catalog and recommendation system streamline the process of choosing and operating tools.

Due to the tool catalogue and the tool recommendation system, small IT firms' owners are able to identify the most suitable tools for their operating environment without spending much time and without having knowledge on all of the open-source tools. By reducing the need for users to choose tools through process of trial and error, the recommendation system's integration offers an additional degree of convenience. The system made sure that users received recommendations that were customized to meet their unique needs by integrating platform compatibility and user goals into the recommendation algorithm. Cybersecurity experts can quickly recognize tools that not only satisfy technical specifications but also fit with organizational objectives and security priorities due to this personalized approach.

4.3.1 Features and Benefits of the Model Framework

In order to enhance security posture of the cloud based small IT firms, the model framework has several key features. By providing a methodical, automated and transparent approach to tool selection, the cybersecurity tool catalog and recommendation system aims to assist cloud-based small IT firms in navigating the complex landscape of cybersecurity solutions. This framework ensures compatibility, effectiveness, and flexibility in response to new threats in addition to classifying and recommending security solutions. It offers a workable, scalable, and affordable way to improve security postures by tackling the main cybersecurity issues that small IT firms face. This framework's intelligent tool recommendation engine is a key component that helps companies in choosing the best cybersecurity tools for their particular requirements. Instead of generic tool lists, this recommendation system makes use of context-aware algorithms that take into account about security threats, compliance requirements, and operating system compatibility (e.g., GDPR, ISO 27001, Windows Server 2022, Kali Linux, and CentOS Stream). This ensures that small IT firms don't spend time and money trying out products that might not be in line with their security objectives.

Additionally, the framework has a dynamically updated tool catalog that is always being updated to represent the most recent information for cybersecurity solutions. Businesses can easily choose and implement the best solutions due to the thorough descriptions, use cases, platform compatibility, and installation instructions provided by each tool entry.

From the perspective of cost-effectiveness, this model helps companies in finding high-impact, inexpensive open-source security solutions instead of using pricey enterprise technologies. Hence, they can maintain businesses' security posture with a higher level of security.

4.3.2 Success of the Model Framework

For cloud-based small IT firms, the cybersecurity tool catalog and recommendation system has shown to be a useful resource, significantly improving the effectiveness and productivity of cybersecurity tool implementation and selection. The framework

has made it possible for companies to strengthen their security postures with less time, money, and effort by simplifying the process of finding and implementing security solutions.

The framework's capacity to accelerate the cybersecurity tool selection procedure is among its most remarkable achievements. When choosing security technologies, companies with specialized cybersecurity teams previously had to deal with time-consuming research, trial-and-error implementations, and compatibility problems. By offering evaluated solutions, the framework removes these obstacles and ensures that companies can quickly install and operate tools that suit their infrastructure, compliance requirements, and threat landscape. As proven in the 4.2 section, the model framework was able to achieve 98% user satisfaction level.

4.3.3 Efficiency Comparison

The selection and operation of cybersecurity tools with and without the framework are compared in this section. The analysis demonstrates the observable advantages of using a structured recommendation system over traditional manual selection techniques by looking at important efficiency indicators including expertise knowledge, cost, time spent and resources of the tools.

Table 5: Efficiency Comparison of the Framework

Metrics	**Traditional Tools Selection Process**	**Process with the Model Framework**
Expertise Knowledge	The user should be expertise in the cybersecurity filed and about the cyber security tools. Limited to known tools by cybersecurity expertise.	Expertise Knowledge is not required to find the most suitable tools.

Cost	Cyber Security budget should be allocated for the following tasks. 1. To hire expertise in cyber security filed 2. For trying out different tools both open source and premium solutions. 3. Unnecessary tool purchases.	Inexpensive process due to the following reasons. 1. Do not need expertise knowledge to select and configure tools. 2. No unnecessary tool purchases and not required to assess the tools. 3. Free open source available.
Time Spent	Based on the cyber security team, it may require days to find the suitable tools.	Within a few minutes, users are able to get the suitable tools for their environment.
Resources of the tools	Available in different websites,	Available in a centralized tool catalogue

4.4 Chapter Summary

This chapter summarized the main conclusions drawn from the development, established and evaluation of the suggested open-source tool-based cybersecurity framework for small IT firms. For the evaluation of the suggested framework and tool catalogue, feedbacks from the industry experts were collected. The results demonstrated that the suggested open-source tools for different environments are considerable. The main characteristics of the suggested model framework were examined in this section, which also included a comparison between the model-driven approach and the traditional tool selection procedure. The discussion section critically analyzed how the results fit the study's goals and the knowledge gained from earlier studies. The results support the literature that highlights the open-source solutions' operational fit, flexibility, and affordability for small IT firms.

CHAPTER 5

CONCLUSIONS AND FURTHER RESEARCH AREAS

5.1 Introduction

Small IT firms are becoming prime targets for the hackers due to their lack of cyber security controls. Nowadays, most of the small IT firms are rely on cloud-based solutions. Despite the fact that open-source cybersecurity tools can be economical and effective for safeguarding their systems, small IT firms may not aware about these open-source cyber security solutions available. Hence, the primary objective of this research is to provide an open-source tool based cyber security framework for small IT firms to overcome their security challenges and improve their security posture.

5.2 Conclusions

Cloud based small IT firms face several cybersecurity issues because they are more vulnerable to cyber-attacks due to lack of cybersecurity controls that are implemented. Their increased risk is exacerbated by inadequate cyber security budget, lack of awareness, and misconfigured systems. These may lead to financial and reputational fallout from a cyber-attack which can be disastrous. In order to overcome this problem, an open-source cyber security tool-based model framework was suggested.

As the first step in this study, the researcher distributed a survey for cloud based small IT firms to find the cyber security challenges they face. The researcher only considered two types of companies.

a) Small IT firms who are handling healthcare related businesses data.

b) Small IT firms who are handling retail businesses data.

The survey distributed among 70 companies and only 44% response rate could achieve as explained in 4.1 section. The survey analysis revealed that the challenges that that small IT firms confront are insufficient password security controls, insufficient access

control mechanisms with MFA and VPN access, not having cyber security awareness trainings, poor policy implementations and compliance controls.

After considering these cyber security challenges, open-source cyber security tools were selected for each challenge and altogether 96 open-source tools were analyzed for features and compatibility of the tool under 11 categories as mentioned in the 3.2.1 section such as access control tools, password management tools, policy management tools, etc. A dataset was prepared based on the gathered information and it was used to train the recommendation system that was implemented for suggesting the most suitable open-source cyber security solutions for the cloud based small IT firms.

For cloud-based small IT firms, the cybersecurity tool catalog and recommendation system are the main components of this framework and has shown to be a successful solution to the challenges of selecting, implementing, and operating security solutions. The framework facilitates users to easily discover necessary open-source tools by providing centralized tools catalogue and generates the most suitable open-source tools for different categories with the recommendation system. In order to evaluate the model framework, cyber security industry experts were involved and provided their feedbacks on tool suggestions as explained in the section 4.2. The recommendation system uses content-based filtering method and evaluated by collecting the industry experts' feedback using Precision at K method. According to those collected feedbacks, the recommendation system could achieve 98% user satisfaction level.

With the help of this framework, which provides customized, contextual suggestions based on their particular needs, infrastructure, and security goals, businesses can easily navigate to the open-source cybersecurity tools. Furthermore, this model framework has tool information with key features, download/ installation guidance, documentation resources, and usage guidance. The framework significantly decreases down on the time and effort needed to find the best tools by automating the recommendation process and offering pre-screened, compatibility-tested selections. This simplified method ensures that the tools selected are ideal for the particular environment while assisting businesses in avoiding the common problems of compatibility, vendor mismatches, and trial-and-error testing.

5.3 Limitations and Further Research Areas

In this study, only two types of cloud based small IT firms are considered

- Small IT firms who are handling healthcare related businesses data
- Small IT firms who are handling retail businesses data.

Different industries may require special concern for various environmental requirements. Hence, the scope could be broadened by investigating other types of small IT firms in order to confirm and improve the open-source tools based cyber security framework.

The implemented framework only includes 96 open-source cyber security tools under 11 categories such as, Access Control Tools, Ticketing Tools, Password Storing and Sharing Tools, Secure Document Sharing and Policy Management Tools, Incident Management Tools, VPN Solutions, Web Application Firewalls (WAF), Phishing Simulation Tools, Code Security Checking Tools- Git, Anti-Malware Tools, Security Awareness - Video quiz creation Platforms, and Security Assessments and Auditing Tools. Beyond these categories, there could be many areas that other industries may devote their attention on. Hence, the future researches need to consider other industries and more open-source tools analysis for future developments.

Threat intelligence also can be considered as another important area that could be included in the future works. The act of gathering, evaluating, and applying data regarding current or anticipated cyberthreats in order to enhance security defenses and make well-informed decisions is known as threat intelligence. It is essential because it aids companies in anticipating risks, comprehending the actions of attackers, and improving their ability to counter threats. Threat intelligence is becoming a critical component of modern cybersecurity methods as cyberattacks get more complicated. As the framework would be better equipped to offer more dynamic and real-time tool suggestions based on their features, incorporating threat intelligence could be viewed as a worthwhile area for future research in the context of this study.

In this study, the researcher only considered about standards such as HIPAA, GDPR, SOC2 and certification requirements for cyber essentials certification. Hence, it can be broadened to consider other cyber security standards such as NIST CSF, PCI DSS, CIS Controls, etc. Furthermore, integration capabilities with the tools such as G-Suite,

GitHub, Jira and Slack were considered in this research and yet, other tools also can be considered as the future works.

During the testing stage, certain restrictions were followed. Even though the recommendation engine offered extremely relevant solutions for the majority of use cases, there could be occasions when users are overly specific, particularly for customers with complicated or unique security needs. More dynamic feedback mechanisms could be incorporated into future iterations of the system to enable the recommendation engine to change in response to user input and new developments in cybersecurity.

REFERENCES

[1]. Watad, M., Washah, S. and Perez, C. (no date) It Security Threats and Challenges for Small Firms: Managers' Perceptions. thesis. International Journal of the Academic Business World . Spring2018, Vol. 12 Issue 1, p23-30. 8p.

[2]. Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020).

[3]. Ramachandra, Gururaj & Iftikhar, Mohsin & Khan, Farrukh. (2017). A Comprehensive Survey on Security in Cloud Computing. Procedia Computer Science. 110. 465-472. 10.1016/j.procs.2017.06.124.

[4]. J. Hayes and A. Bodhani, "Cyber security: small firms under fire [InformatIon Technology Professionalism]," in Engineering & Technology, vol. 8, no. 6, pp. 80-83, July 2013, doi: 10.1049/et.2013.0614.

[5]. C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell and M. N. Bashir, "Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, HI, USA, 2017, pp. 50-57, doi: 10.1109/CLOUD.2017.16.

[6]. Tariq, M.I. (2012) Towards Information Security Metrics Framework for Cloud Computing. International Journal of Cloud Computing and Services Science (IJ-CLOSER).

[7]. Akashdeep Bhardwaj and Sam Goundar (2019) A framework to define the relationship between Cyber Security and Cloud Performance, Computer Fraud & Security. Elsevier. Available at: https://www.sciencedirect.com/science/article/abs/pii/S136137231930020X (Accessed: February 12, 2023).

[8]. Rupra, Satwinder & Omamo, Amos. (2020). A Cloud Computing Security Assessment Framework for Small and Medium Enterprises. Journal of Information Security. 11. 201-224. 10.4236/jis.2020.114014.

[9]. Chidukwani, A., Zander, S. and Koutsakis, P. (2022) A survey on the cyber security of Small-to-Medium businesses: Challenges, research focus and recommendations. IEEE Access, 10 . pp. 85701-85719.

[10]. Syafrizal, M., Selamat, S. R. and Zakaria, N. A. (2022) "Analysis of Cybersecurity Standard and Framework Components", International Journal of Communication Networks and Information Security (IJCNIS), 12(3). doi: 10.17762/ijcnis.v12i3.4817.

[11]. Tissir, Najat & El Kafhali, Said & Aboutabit, Noureddine. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. Journal of Reliable Intelligent Environments. 10.1007/s40860-020-00115-0.

[12]. Raghavan, Kamala. (2017). Managing cybersecurity and e-commerce risks in small businesses. Journal of Management Science and Business Intelligence. 2. 9-15. 10.5281/zenodo.581691.

[13]. T. Tam, A. Rao, J. Hall The good, the bad and the missing: a Narrative review of cyber-security implications for australian small businesses Comput. Secur., 109 (2021), Article 102385, 10.1016/j.cose.2021.102385

[14]. H. Gupta and D. Kumar, "Security Threats in Cloud Computing," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 2019, pp. 1158-1162, doi: 10.1109/ICCS45141.2019.9065542.

[15]. Angelo Furfaro, Antonio Piccolo, Andrea Parise, Luciano Argento, and Domenico Saccà. 2018. A Cloud-based platform for the emulation of complex cybersecurity scenarios. Future Gener. Comput. Syst. 89, C (Dec 2018), 791–803. https://doi.org/10.1016/j.future.2018.07.025

[16]. Almatari, Osamah & Helal, Iman & Mazen, Sherif & Elhennawy, Sherif. (2018). Cybersecurity Tools for IS Auditing. 10.1109/ES.2018.00040.

[17]. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. Journal of Organizational Computing and Electronic Commerce, 28, 269 - 282.

[18]. Li, Yanyan & Nguyen, Dung & Xie, Mengjun. (2017). EZSetup: A Novel Tool for Cybersecurity Practices Utilizing Cloud Resources. 53-58. 10.1145/3125659.3125699.

[19]. Kaila, Urpo. “Information Security Best Practices: First Steps for Startups and SMEs.” Technology Innovation Management Review (2018): n. pag.

[20]. Lee, In. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons. 64. 10.1016/j.bushor.2021.02.022.

[21]. 2022 data breach investigations report (2022) Verizon Business. Available at: https://www.verizon.com/business/resources/reports/dbir/ (Accessed: February 10, 2023).

[22]. Miller, G. (2017) 60% of small companies that suffer a cyber attack are out of business within six months., The Denver Post. The Denver Post. Available at: https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/ (Accessed: February 10, 2023).

[23]. Cook, K.D., 2017. Effective cyber security strategies for small businesses (Doctoral dissertation, Walden University).

[24]. Le, N.T. and Hoang, D.B., 2017. Capability maturity model and metrics framework for cyber cloud security. Scalable Computing.

[25]. Xie, N., Mead, N.R., Chen, P., Dean, M., Lopez, L., Ojoko-Adams, D. and Osman, H., 2004. SQUARE project: Cost/benefit analysis framework for information security improvement projects in small companies.

[26]. Alshboul, Y. and Streff, K., 2015. Analyzing information security model for small-medium sized businesses.

[27]. Tariq, M.I., Tayyaba, S., Hashmi, M.U., Ashraf, M.W. and Mian, N.A., 2017. Agent based information security threat management framework for hybrid cloud computing. IJCSNS, 17(12), p.57.

[28]. Sheehan, B., Murphy, F., Kia, A.N. and Kiely, R., 2021. A quantitative bow-tie cyber risk classification and assessment framework. Journal of Risk Research, 24(12), pp.1619-1638.

[29]. McLilly, L. and Qu, Y., 2020, December. Quantitatively Examining Service Requests of a Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses. In 2020 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 116-121). IEEE.

[30]. Babalola, A.O., 2021. Effective Strategies for Cybersecurity and Information Technology Governance for Small Business Leaders: A Quantitative Study (Doctoral dissertation, University of Phoenix).

[31]. Udofot, M. and Topchyan, R., 2020. Factors related to small business cyber-attack protection in the United States. International Journal of Cyber-Security and Digital Forensics, 9(1), pp.12-25.

[32]. Gai, K., Qiu, M. and Hassan, H., 2017. Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud

computing. Concurrency and Computation: Practice and Experience, 29(7), p.e3856.

[33]. Binu, M.S. and Meenakumari, J., 2012. A security framework for an enterprise system on cloud. Indian Journal of Computer Science and Engineering (IJCSE), 3(4), pp.548-552.

[34]. Elzamly, A., Hussin, B., Abu Naser, S., Khanfar, K., Doheir, M., Selamat, A. and Rashed, A., 2016. A new conceptual framework modelling for cloud computing risk management in banking organizations. International Journal of Grid and Distributed Computing, 9(9), pp.137-154.

[35]. Gai, K., Qiu, M. and Elnagdy, S.A., 2016, April. A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) (pp. 171-176). IEEE.

[36]. Mehraj, S. and Banday, M.T., 2020, January. Establishing a zero trust strategy in cloud computing environment. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-6). IEEE.

[37]. Khaleefah, A.D. and Al-Mashhadi, H.M., 2023. Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review. Int. J. Wirel. Microw. Technol, 13, pp.1-13.

[38]. Sakr, A., Yaacoub, E., Noura, H., Al-Husseini, M., Abualsaud, K., Khattab, T. and Guizani, M., 2018, April. A secure client-side framework for protecting the privacy of health data stored on the cloud. In 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM) (pp. 1-6). IEEE.

[39]. Chang, V., Kuo, Y.H. and Ramachandran, M., 2016. Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, pp.24-41.

[40]. Mansfield-Devine, S., 2016. Securing small and medium-size businesses. Network Security, 2016(7), pp.14-20.

[41]. Yadav, A., Kumar, A. and Singh, V., 2023. Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. Artificial Intelligence Review, pp.1-32.

[42]. Kumar, R. and Goyal, R., 2020. Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC). Computers & Security, 97, p.101967.

[43]. Berger, H. and Jones, A., 2016, July. Cyber security & ethical hacking for SMEs. In Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society (pp. 1-6)

[44]. Adekotujo, A., Odumabo, A., Adedokun, A. and Aiyeniko, O., 2020. A comparative study of operating systems: Case of windows, unix, linux, mac,

android and ios. International Journal of Computer Applications, 176(39), pp.16-23.

[45]. Javed, U., Shaukat, K., Hameed, I.A., Iqbal, F., Alam, T.M. and Luo, S., 2021. A review of content-based and context-based recommendation systems. International Journal of Emerging Technologies in Learning (iJET), 16(3), pp.274-306.

APPENDICES

Appendix A: Dataset

Category 1: Access Control Tools List

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health care_ busin	retail _busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ra	inte_ji lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
2	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 MidPoint
3	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 keycloak
4	Access control	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1 OpenAM
5	Access control	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 Gluu Server
6	Access control	1	1		1	1	1		1	1	1					1	1	1	1	1 Wren AM
7	Access control	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 Apache Syncope
8	Access control	1	1	1	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	1 CAS
9	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 OpenIAM
10	Access control	1	1	1	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	1 Ory Kratos
11	Access control	1	1	1	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	1 Authelia
12	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 Authentik
13	Access control	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1 FusionAuth
14	Access control	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 osTicket
15	Access control	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 Zammad
16	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 OTRS
17	Access control	0	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	1	1	0 Request Tracker
18	Access control	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Faveo Helpdesk
19	Access control	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0 Helpy
20	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 Uvdesk
21	Access control	0	1	1	1	1	1	0	1	1	1	0	0	0	0	0	0	1	1	0 Redmine
22	Access control	0	1	1	1	1	1	0	1	1	1	0	0	0	0	0	0	1	1	0 MantisBT
23	Access control	0	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0 GLPI
24	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 Auth0
25	Access control	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1 Orv Hvdra

Category 2: Password Management Tools List

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_business	retail_business	has_updates	com_support	cost_free	useWith_Internal	user_friendliness	comp_linux	comp_windows	comp_centos	inte_gsuite	inte_github	inte_jira	inte_slack	is_comply_hipaa	is_comply_gdpr	is_comply_Cyber	is_comply_SOC2	selected_tool
26	Password mana	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Bitwarden
27	Password mana	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	KeePass
28	Password mana	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Passbolt
29	Password mana	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Teampass
30	Password mana	1	1	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Psono
31	Password mana	1	1	1	0	1	1	1	1	0	1	0	0	0	0	1	1	1	1	Padlock

Category 3: Policy Management Tools List

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health care_ busin	retail _busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ji ra	inte_s lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
32	Policy Manager	1	1	1	0	1	1	0	1	0	1	0	0	0	0	1	1	1	1	1 Vaultier
33	Policy Manager	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 Cryptomator
34	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Papermerge
35	Policy Manager	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 Teedy
36	Policy Manager	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1 OpenDocMan
37	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 OpenKM
38	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Nextcloud
39	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Syncthing
40	Policy Manager	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	0	1	1 VeraCrypt
41	Policy Manager	1	1	1	1	1	1	1	0			0	0	0	0	1	1	1	1	1 PeaZip
42	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Seafile
43	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Docspell
44	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 ONLYOFFICE
45	Policy Manager	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0 Etherpad
46	Policy Manager	1	1		1	1	1	1	1		1	0	0	0	0	1	1	1	1	1 DigiDocu
47	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 DokuWiki
48	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 MediaWiki
49	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Alfresco Community Edition
50	Policy Manager	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1 Mayan EDMS
51	Policy Manager	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1 Paperless-ngx

Category 4: Incident Response Tools List

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_busin	retail_busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ji ra	inte_s lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
52	Incident Respor	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	TheHive
53	Incident Respor	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Cortex
54	Incident Respor	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	GRR Rapid Response
55	Incident Respor	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	DFIR-IRIS
56	Incident Respor	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	OSSEC
57	Incident Respor	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	OSSIM
58	Incident Respor	1	1	1	1	1	1	0	1	0	1	0	0	0	0	1	1	1	1	osquery
59	Incident Respor	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	Cyphon

Category 5: VPN Solutions

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_business	retail_business	has_updates	com_support	cost_free	useWithErnal	user_friendlyness	comp_linux	comp_windows	comp_centos	inte_gsuite	inte_github	inte_jira	inte_slack	is_comply_hipaa	is_comply_gdpr	is_comply_Cyber	is_comply_SOC2	selected_tool
60	VPN Solutions	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	OpenVPN
61	VPN Solutions	1	1	1	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	WireGuard
62	VPN Solutions	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	SoftEther VPN
63	VPN Solutions	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Libreswan
64	VPN Solutions	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	StrongSwan
65	VPN Solutions	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	Freelan
66	VPN Solutions	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	Algo VPN

Category 6: WAF Solutions

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health care_ busin	retail _busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ji ra	inte_s lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
67	WAF Solutions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	ModSecurity
68	WAF Solutions	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	NAXSI
69	WAF Solutions	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	IronBee
70	WAF Solutions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	open-appsec
71	WAF Solutions	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	CloudFlare Free Plan
72	WAF Solutions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	OWASP Coraza
73	WAF Solutions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Vulture
74	WAF Solutions	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	WebKnight

Category 7: Phishing Simulation Tools

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_business	retail_business	has_updates	com_support	cost_free	useWith_Internal	user_friendliness	comp_linux	comp_windows	comp_centos	inte_gsuite	inte_github	inte_jira	inte_slack	is_comply_hipaa	is_comply_gdpr	is_comply_Cyber	is_comply_SOC2	selected_tool
75	Phishing simula	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	GoPhish
76	Phishing simula	1	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1	King Phisher
77	Phishing simula	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	Modlishka

Category 8: Code Security checking tools - GitHub

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health care_ busin	retail _busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ji ra	inte_s lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
78	Code Security cl	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	SAP Credential Digger
79	Code Security cl	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	trufflehog
80	Code Security cl	1	1	1	1	1	1	1	0			1	1	1	1	1	1	1	1	SOOS

Category 9: Anti- Malware Tools

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_business	retail_business	has_updates	com_support	cost_free	useWith_Internal	user_friendliness	comp_linux	comp_windows	comp_central os	inte_g suite	inte_github	inte_jira	inte_slack	is_comply_hipaa	is_comply_gdpr	is_comply_Cyber	is_comply_SOC2	selected_tool
81	Anti-malware	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	ClamTk
82	Anti-malware	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Comodo Antivirus
83	Anti-malware	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Sophos Home Free
84	Anti-malware	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Malwarebytes

Category 10: Awareness Implementation Platforms

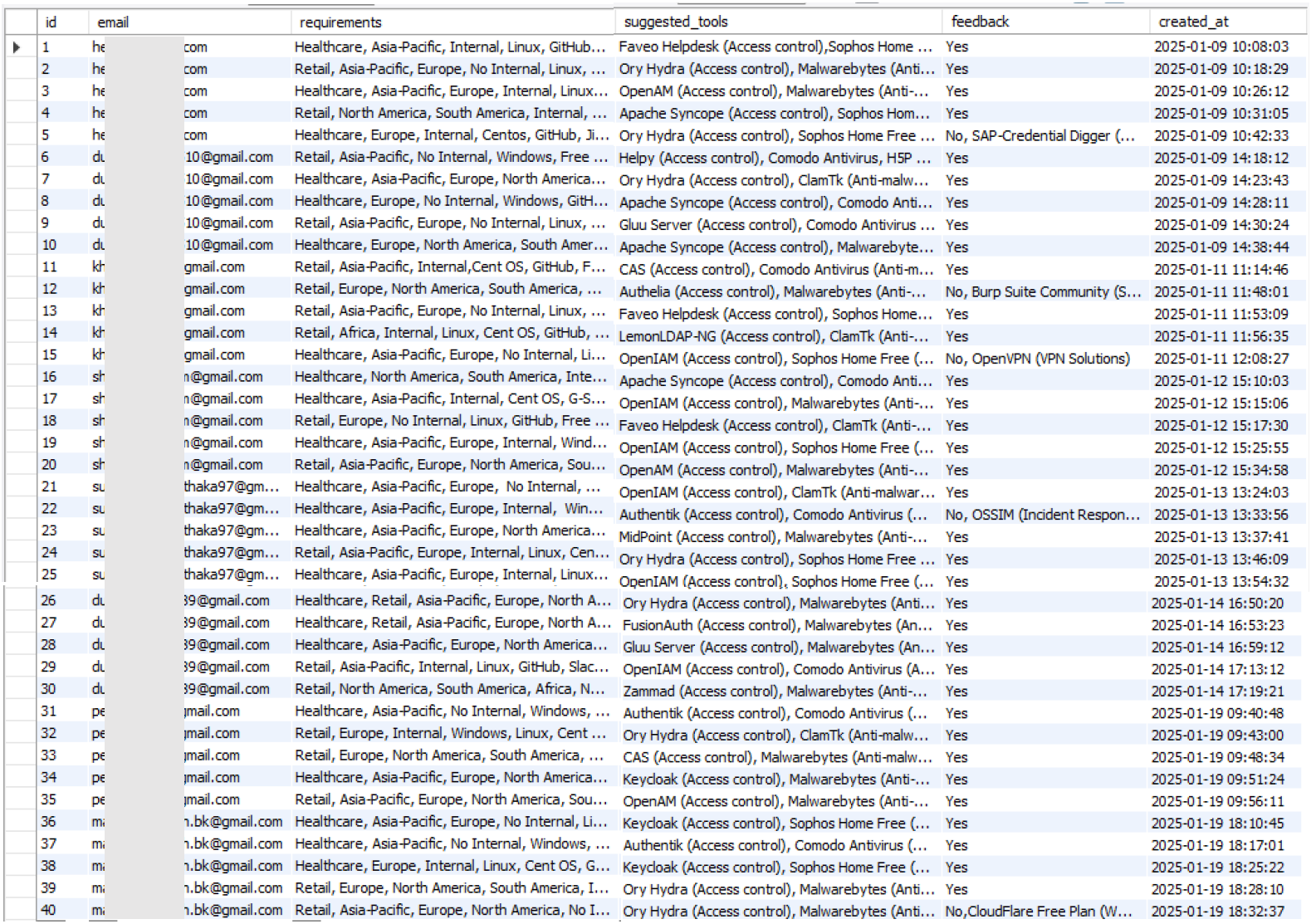
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health_care_business	retail_business	has_updates	com_support	cost_free	useWith_Internal	user_friendliness	comp_linux	comp_windows	comp_central_os	inte_gsuite	inte_github	inte_jira	inte_slack	is_comply_hipaa	is_comply_gdpr	is_comply_Cyber	is_comply_SOC2	selected_tool
85	Awareness impl	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	H5P
86	Awareness impl	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	ILIAS
87	Awareness impl	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Open edX

Category 11: Security Assessment and Audit Tools

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	tool_category	health care_ busin	retail _busi ness	has_u pdate s	com_s uppor t	cost_f ree	useWi th_Int ernal	user_f riendl yness	comp _linux	comp _wind ows	comp _cent os	inte_g suite	inte_g ithub	inte_ji ra	inte_s lack	is_co mply_ hipaa	is_co mply_ gdpr	is_co mply_ Cyber	is_co mply_ SOC2	selected_tool
88	Security assessr	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Burpsuite Community
89	Security assessr	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	OWASP ZAP
90	Security assessr	1	1	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	Web Check
91	Security assessr	1	1	1	0	1	0	1	0	0	0	1	1	1	1	1	1	1	1	Shodan
92	Security assessr	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	CIS CSAT
93	Security assessr	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	OpenVAS
94	Security assessr	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	Prowler
95	Security assessr	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Tripwire
96	Security assessr	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	Open-Audit
97	Security assessr	1	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	Lynis

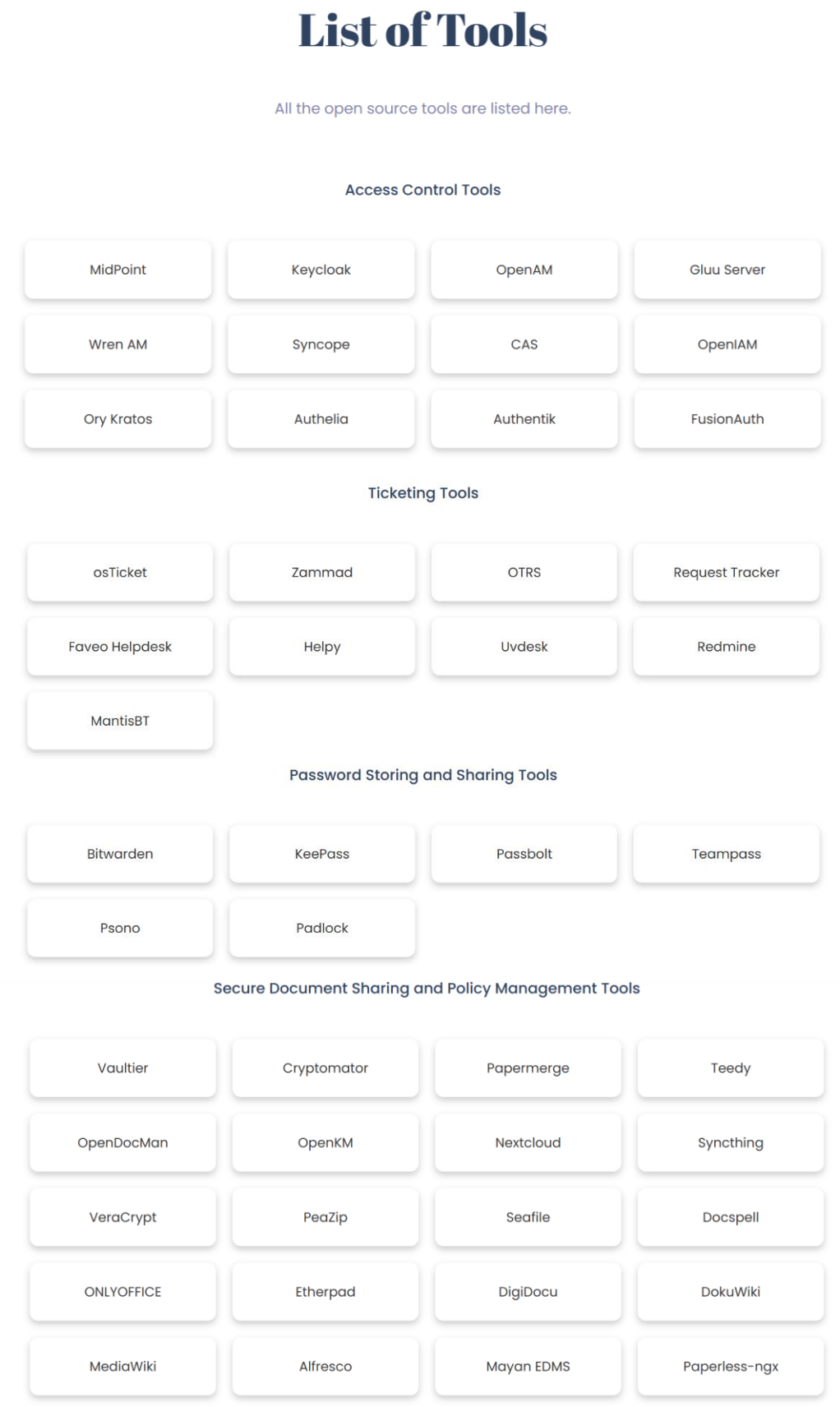
Appendix B: Evaluation Results of the Recommendation System (Summarized)

Email	Response 1	Response 2	Response 3	Response 4	Response 5
he[redacted]com	Yes	Yes	Yes	Yes	User Preferences: - Code-security: SAP Credential Digger - Anti-malware: Malwarebytes
du[redacted]10@gmail.com	Yes	Yes	Yes	Yes	Yes
kh[redacted]gmail.com	Yes	No User Preferences: - Security-assessment: Burpsuite Community	Yes	Yes	User Preferences: - Vpn: OpenVPN
sh[redacted]@gmail.com	Yes	Yes	Yes	Yes	Yes
su[redacted]haka97@gmail.com	Yes	User Preferences: - Incident-response: OSSIM	Yes	Yes	Yes
du[redacted]9@gmail.com	Yes	Yes	Yes	Yes	Yes
pe[redacted]mail.com	Yes	Yes	Yes	Yes	Yes
m[redacted].bk@gmail.com	Yes	Yes	Yes	Yes	User Preferences: - Waf: CloudFlare Free Plan



id	email	requirements	suggested_tools	feedback	created_at
1	he com	Healthcare, Asia-Pacific, Internal, Linux, GitHub...	Faveo Helpdesk (Access control),Sophos Home ...	Yes	2025-01-09 10:08:03
2	he com	Retail, Asia-Pacific, Europe, No Internal, Linux, ...	Ory Hydra (Access control), Malwarebytes (Anti...	Yes	2025-01-09 10:18:29
3	he com	Healthcare, Asia-Pacific, Europe, Internal, Linux...	OpenAM (Access control), Malwarebytes (Anti-...	Yes	2025-01-09 10:26:12
4	he com	Retail, North America, South America, Internal, ...	Apache Syncope (Access control), Sophos Hom...	Yes	2025-01-09 10:31:05
5	he com	Healthcare, Europe, Internal, Centos, GitHub, Ji...	Ory Hydra (Access control), Sophos Home Free ...	No, SAP-Credential Digger (...	2025-01-09 10:42:33
6	du 10@gmail.com	Retail, Asia-Pacific, No Internal, Windows, Free ...	Helpy (Access control), Comodo Antivirus, H5P ...	Yes	2025-01-09 14:18:12
7	du 10@gmail.com	Healthcare, Asia-Pacific, Europe, North America...	Ory Hydra (Access control), ClamTk (Anti-malw...	Yes	2025-01-09 14:23:43
8	du 10@gmail.com	Healthcare, Europe, No Internal, Windows, GitH...	Apache Syncope (Access control), Comodo Anti...	Yes	2025-01-09 14:28:11
9	du 10@gmail.com	Retail, Asia-Pacific, Europe, No Internal, Linux, ...	Gluu Server (Access control), Comodo Antivirus ...	Yes	2025-01-09 14:30:24
10	du 10@gmail.com	Healthcare, Europe, North America, South Amer...	Apache Syncope (Access control), Malwarebyte...	Yes	2025-01-09 14:38:44
11	kh gmail.com	Retail, Asia-Pacific, Internal,Cent OS, GitHub, F...	CAS (Access control), Comodo Antivirus (Anti-m...	Yes	2025-01-11 11:14:46
12	kh gmail.com	Retail, Europe, North America, South America, ...	Authelia (Access control), Malwarebytes (Anti-...	No, Burp Suite Community (S...	2025-01-11 11:48:01
13	kh gmail.com	Retail, Asia-Pacific, Europe, No Internal, Linux, ...	Faveo Helpdesk (Access control), Sophos Home...	Yes	2025-01-11 11:53:09
14	kh gmail.com	Retail, Africa, Internal, Linux, Cent OS, GitHub, ...	LemonLDAP-NG (Access control), ClamTk (Anti-...	Yes	2025-01-11 11:56:35
15	kh gmail.com	Healthcare, Asia-Pacific, Europe, No Internal, Li...	OpenIAM (Access control), Sophos Home Free (...	No, OpenVPN (VPN Solutions)	2025-01-11 12:08:27
16	sh n@gmail.com	Healthcare, North America, South America, Inte...	Apache Syncope (Access control), Comodo Anti...	Yes	2025-01-12 15:10:03
17	sh n@gmail.com	Healthcare, Asia-Pacific, Internal, Cent OS, G-S...	OpenIAM (Access control), Malwarebytes (Anti-...	Yes	2025-01-12 15:15:06
18	sh n@gmail.com	Retail, Europe, No Internal, Linux, GitHub, Free ...	Faveo Helpdesk (Access control), ClamTk (Anti-...	Yes	2025-01-12 15:17:30
19	sh n@gmail.com	Healthcare, Asia-Pacific, Europe, Internal, Wind...	OpenIAM (Access control), Sophos Home Free (...	Yes	2025-01-12 15:25:55
20	sh n@gmail.com	Retail, Asia-Pacific, Europe, North America, Sou...	OpenAM (Access control), Malwarebytes (Anti-...	Yes	2025-01-12 15:34:58
21	su thaka97@gm...	Healthcare, Asia-Pacific, Europe, No Internal, ...	OpenIAM (Access control), ClamTk (Anti-malwar...	Yes	2025-01-13 13:24:03
22	su thaka97@gm...	Healthcare, Asia-Pacific, Europe, Internal, Win...	Authentik (Access control), Comodo Antivirus (...	No, OSSIM (Incident Respon...	2025-01-13 13:33:56
23	su thaka97@gm...	Healthcare, Asia-Pacific, Europe, North America...	MidPoint (Access control), Malwarebytes (Anti-...	Yes	2025-01-13 13:37:41
24	su thaka97@gm...	Retail, Asia-Pacific, Europe, Internal, Linux, Cen...	Ory Hydra (Access control), Sophos Home Free ...	Yes	2025-01-13 13:46:09
25	su thaka97@gm...	Healthcare, Asia-Pacific, Europe, Internal, Linux...	OpenIAM (Access control), Sophos Home Free (...	Yes	2025-01-13 13:54:32
26	du 39@gmail.com	Healthcare, Retail, Asia-Pacific, Europe, North A...	Ory Hydra (Access control), Malwarebytes (Anti...	Yes	2025-01-14 16:50:20
27	du 39@gmail.com	Healthcare, Retail, Asia-Pacific, Europe, North A...	FusionAuth (Access control), Malwarebytes (An...	Yes	2025-01-14 16:53:23
28	du 39@gmail.com	Healthcare, Asia-Pacific, Europe, North America...	Gluu Server (Access control), Malwarebytes (An...	Yes	2025-01-14 16:59:12
29	du 39@gmail.com	Retail, Asia-Pacific, Internal, Linux, GitHub, Slac...	OpenIAM (Access control), Comodo Antivirus (A...	Yes	2025-01-14 17:13:12
30	du 39@gmail.com	Retail, North America, South America, Africa, N...	Zammad (Access control), Malwarebytes (Anti-...	Yes	2025-01-14 17:19:21
31	pe mail.com	Healthcare, Asia-Pacific, No Internal, Windows, ...	Authentik (Access control), Comodo Antivirus (...	Yes	2025-01-19 09:40:48
32	pe mail.com	Retail, Europe, Internal, Windows, Linux, Cent ...	Ory Hydra (Access control), ClamTk (Anti-malw...	Yes	2025-01-19 09:43:00
33	pe mail.com	Retail, Europe, North America, South America, ...	CAS (Access control), Malwarebytes (Anti-malw...	Yes	2025-01-19 09:48:34
34	pe mail.com	Healthcare, Asia-Pacific, Europe, North America...	Keycloak (Access control), Malwarebytes (Anti-...	Yes	2025-01-19 09:51:24
35	pe mail.com	Retail, Asia-Pacific, Europe, North America, Sou...	OpenAM (Access control), Malwarebytes (Anti-...	Yes	2025-01-19 09:56:11
36	ma n.bk@gmail.com	Healthcare, Asia-Pacific, Europe, No Internal, Li...	Keycloak (Access control), Sophos Home Free (...	Yes	2025-01-19 18:10:45
37	ma n.bk@gmail.com	Healthcare, Asia-Pacific, No Internal, Windows, ...	Authentik (Access control), Comodo Antivirus (...	Yes	2025-01-19 18:17:01
38	ma n.bk@gmail.com	Healthcare, Europe, Internal, Linux, Cent OS, G...	Keycloak (Access control), Sophos Home Free (...	Yes	2025-01-19 18:25:22
39	ma n.bk@gmail.com	Retail, Europe, North America, South America, I...	Ory Hydra (Access control), Malwarebytes (Anti...	Yes	2025-01-19 18:28:10
40	ma n.bk@gmail.com	Retail, Asia-Pacific, Europe, North America, No I...	Ory Hydra (Access control), Malwarebytes (Anti...	No,CloudFlare Free Plan (W...	2025-01-19 18:32:37

Appendix C: Tool Catalogue



Incident Response Tools

TheHive	Cortex	GRR Rapid Response	DFIR-IRIS
OSSEC	OSSIM	osquery	Cyphon

VPN Solutions

OpenVPN	WireGuard	SoftEther VPN	Libreswan
StrongSwan	Freelan	Algo VPN	

Web Application Firewalls (WAFs)

ModSecurity	NAXSI	IronBee	open-appsec
CloudFlare Free Plan	OWASP Coraza	Vulture	WebKnight

phishing simulation tools

GoPhish	King Phisher	Modlishka

Code Security for Github

SAP-Credential Digger	trufflehog	SOOS

Anti-Malware tools

ClamTk	Comodo Antivirus	Sophos Home Free	Malwarebytes

Security Awareness - Video quiz creation Platforms

H5P	ILIAS	Open edX

Security Assessments and Auditing Tools

Burpsuite Community	OWASP ZAP	Web Check	Shodan
CIS CSAT	OpenVAS	Prowler	Tripwire
Open-Audit	Lynis		