UNIVERSITY OF TURKU

Framework for Improving Cybersecurity in Cloud based VoIP provider

Cyber Security

Master's Degree Programme in Information and Communication Technology

Department of Computing, Faculty of Technology

Master of Science in Technology Thesis

Author:

Alan Benny Thomas

Supervisors:

Tahir Mohammad

Petri Sainio

Company Supervisor:

Kalyan Kumar Pasumarthy

June 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Alan Benny Thomas
Title: Framework for Improving Cybersecurity in Cloud based VoIP provider
Number of pages: 50
Date: June 2025

Cloud communication services such as voice calling, video conferencing, and messaging have become vital to both individuals and businesses. As the reliance on cloud-based platforms increases, so does the exposure to cybersecurity threats, including data breaches, brute force attacks, and insider threats. This thesis focuses on examining the current security posture of Moitele, a cloud communication company based in Turku, Finland, with the aim of identifying existing gaps and proposing a framework to enhance its security infrastructure.

To achieve this, the study adopts a single case study approach focused on qualitative insights where a one to one interview was conducted with the CEO where the conversations happened where about understanding and getting a first hand knowledge of security practices, challenges, and future strategies. Instead of formal thematic analysis, the interview responses are presented as a straightforward question and answer format, reflecting the limited data available.

The findings from the interview have showed that the Moitele's security implementation strongly rely on Multi-Factor Authentication (MFA) and data encryption and there is limited awareness of the latest security norms such as Zero Trust principles, AI/ML integration, enhanced incident response, and ongoing employee awareness programs. During the interview, the company also values the latest technologies such as blockchain and automation which they have not yet been adopted yet but may be in the future.

Based on this collected information, the thesis proposes a tailored security framework focusing on Zero Trust principles, AI/ML integration, enhanced incident response, and ongoing employee awareness programs. Even though the results are based on one company, they give useful advice to other small to midsized cloud communication companies who have similar security problems.

Keywords: Cloud communication, cybersecurity, security framework, Zero Trust, case study, Moitele

Table of contents

1 Introduction

Cloud Communication have changed rapidly in the recent years, there has been always an improvement in its evolvement from sending letter to voice calls, texting, video calling, conferencing, etc has evolved with the invention of internet with high dependability and cheap. These services are now necessary for daily operations, especially since the COVID-19 pandemic made people work from home around the world. As the modern businesses completely depend on this cloud platform to work together, the infrastructure that supports these services has increased a lot in size and complexity.

This expansion of these technolgies and its dependency has raised a big range of security concerns, speaking from a Cloud communication perspective, those companies who provides these service often manage sensitive data such as call records, messages, customer details, and internal communications making them a prime target for cyberattacks. The rising number of threats such as data breaches, phishing, brute force assaults, and Distributed Denial of Service (DDoS) attacks shows how important it is to have good security measures. Even though encryption and multi-factor authentication (MFA) are commonly used standards, hackers still find weaknesses, especially in systems that aren't regularly updated or watched.

This thesis explores the current security posture of cloud communication companies through a detailed case study of Moitele, a Finland based telecommunications provider. By investigating Moitele’s existing security practices, employee awareness, and readiness to adopt advanced security models, this research aims to identify gaps and propose a robust security framework. While the findings are drawn from one company’s experience, they reflect broader trends and challenges that apply across the cloud communications sector, especially for small and mid-sized providers.

1.1 Problem statement

Cloud communication companies, which provides various services such as voice calls, text messaging, video conferencing has evolved rapidly and has become an integral part of global connectivity. As evolving, more individuals and businesses relay on cloud-based communication systems for connectivity, the volume of data generated in a day is huge which resulted as the primary target for cyber-attacks, such as data breach, Denial of service (Dos), unauthorised access because of their dependency on these technologies. These cyber-attacks can result in various consequences which includes financial loss, reputational damages, user privacy etc. Even after implementing the latest security measures, due to the evolving cyber

threats, the companies are still facing difficulties, recent reports indicates that data breaches and DoS attacks have significantly increased across cloud-based platforms in recent years, highlighting the need for more robust security frameworks [1][2].

This thesis aim is to develop a strategic framework that helps the cloud communication companies to enhance their current security measures to protect them from potential cyber threats.

1.2 Research question

The research will be answering the following questions

1. What is the current security measure used in the cloud communication companies?
2. What are the different challenges or threats the cloud communication company have faced?
3. How can strategic framework enhance the security measures in cloud communication companies?

1.3 Research objectives

The specific research objective are as follows:

- To identify different types of cyber threats, attacks the company has encountered in its history.
- To identify past security incidents and their effects.
- To propose a strategic security framework that improves safety measures, alongside suggestions for new tools and methods to deal with new cyberthreats in cloud communication settings.

1.4 Thesis organisation

The thesis is divided into six main chapters:

Chapter 1- Introduction: Defining the overview of the research problem, the research questions, the main objective and the structure of the thesis.

Chapter 2- Literature Review: Discussing the existing literature review of the current technologies used in the cloud communication sector, current security measures they are using, the threats companies have encountered.

Chapter 3- Methodology: Describes the methods used in this study, including the analytical approaches and data collection methods (interviews).

Chapter 4- Findings: Summarises the research's findings, including observations from interviews, and security framework evaluations.

Chapter 5- Framework: Proposes a comprehensive security framework based on the findings, recommendations to improve the security posture of cloud communication companies.

Chapter 6- Conclusion and Recommendations: Summarize the findings, discusses their effects, and provides recommendations for future research and practical applications.

Disclaimer on Use of AI Tools and Language Editing

This thesis has been prepared with the aid of certain digital tools to enhance the writing quality and productivity. Specifically, OpenAI’s ChatGPT was used to assist with generating drafts and structuring sections, while Grammarly was utilized for grammar checking and language polishing. The use of these tools was limited to language refinement and did not substitute for critical analysis, originality, or personal contribution to the research findings and conclusions. All substantive content, data analysis, and interpretations reflect the author’s own work and academic integrity.

2 Literature review

2.1 Cloud Communication Technologies

Cloud communication technology, the rapid growing digital interaction technology which includes Voice over internet protocol (VOIP), video conferencing, messaging has increased drastically, due to this evolving technology, it has helped individual and business to connect seamlessly across the world along with cost efficient, scalability and flexibility.

These technologies play a crucial role in the age of digital transformation by utilising cloud infrastructure to offer services that would otherwise be restricted by traditional communications techniques.

There has been a rapid demand of cloud communication post the covid pandemic due to the introduction of work from home strategy which can increased in business for cloud communication providers, which resulted in increased security risk as the company data was transmitted and stored in cloud platforms [3]. Studies shows that Datagram Transport Layer Security (DTLS) and Secure Real-time Transport Protocol (SRTP) are essential for protecting real-time communications against manipulation and interception, However, despite these protocols, cloud communication still faces unique challenges in ensuring end to end security, especially in environments with shared resources [4][5].

2.1.1 Cloud vs. On Premise Communication: A Security Perspective

A crucial distinction exists between cloud and on-premises communication systems, particularly in terms of security, control, and operational responsibilities. On premise systems are hosted internally within an organization's infrastructure, giving administrators full control over hardware, software, network configurations, and compliance enforcement. These systems provide better data sovereignty and are often preferred in industries with stringent regulatory demands. However, maintaining such systems requires dedicated IT staff, significant upfront investment, and ongoing operational costs [13], [38].

Cloud communication systems, on the other hand, are hosted on third party infrastructure and accessed via the internet. They offer benefits such as cost efficiency, rapid scalability, global accessibility, and seamless integration with modern collaboration tools. However, they also present security challenges such as shared tenancy, vendor lock in, and limited visibility into backend operations. Cloud services typically operate under a shared responsibility model where

the provider secures the underlying infrastructure while the client is responsible for user access, data protection, and configuration [39].

A major concern in cloud environments is data residency the physical location of data storage which may be outside a client's jurisdiction, raising compliance issues under regulations like GDPR. Furthermore, misconfigured cloud storage or insecure APIs have become common attack vectors. Gartner (2022) estimated that by 2025, 99% of cloud security failures will be the customer's fault due to misconfigurations or lack of governance [40].

While cloud systems are often updated with the latest security protocols by providers, they require clients to implement robust access control mechanisms such as identity federation, multifactor authentication (MFA), and data encryption. On premises systems, though harder to scale and update, give full visibility and allow for customization of security layers tailored to internal risk management strategies [41].

In summary, the choice between cloud and on premises systems hinge on an organization's need for scalability versus control. Hybrid models are increasingly adopted to combine the flexibility of cloud with the control of on premises setups.

2.2 Security Standards and Practises

Maintaining strong security procedures in cloud communication is essential for protecting user information and ensuring legal compliance. Certain security standards such as ISO/IEC 27001 standard which focus on Information Security Management Systems (ISMS) which helps cloud communication companies in risk management, access management, encryption and incident response, which address potential security vulnerabilities [6].

Along with ISO/IEC 27001, the National Institute of Standard and Technology has also developed a security framework, that helps in managing the security risk in cloud environments. The NIST follows five function strategy which includes Identify, Protect, Detect, Respond and Recover which helps in developing security programs [7]. Adding on, the Cloud Security Alliances (CSA) has also introduced the Cloud Control Matrix (CCM) which is an cyber security framework that focus on all the cloud services and the CCM includes the controls related to Identify and Access Management (IAM) where only authorized users have access to the sensitive data, Encryption which is to protect data at rest and in transit ensuring confidentiality, and finally Threat Intelligence which helps in stay informed of the latest emerging threats and proactively defending them [8].

Regulatory compliance has become important as well, where with the global data privacy regulations which included General Data Protection Regulations(GDPR)[9] and California Consumer Privacy Act (CCPA)[10] where both of these talks about the data protection and privacy has to be their top priority and cloud companies should make sure that necessary implementations needs to be there to ensure this because breaking these rules can result in severe penalties, businesses are adopting frameworks like the CSA's CCM to strengthen their compliance posture.

Finally, with one of the latest emerging architecture Zero Trust Architecture (ZTA), where it follows a principle “never trust anyone, always authenticate” and make sure that continuous verification of users and devices, networks, and strict access controls as preventive measures against data breaches and threats [11].

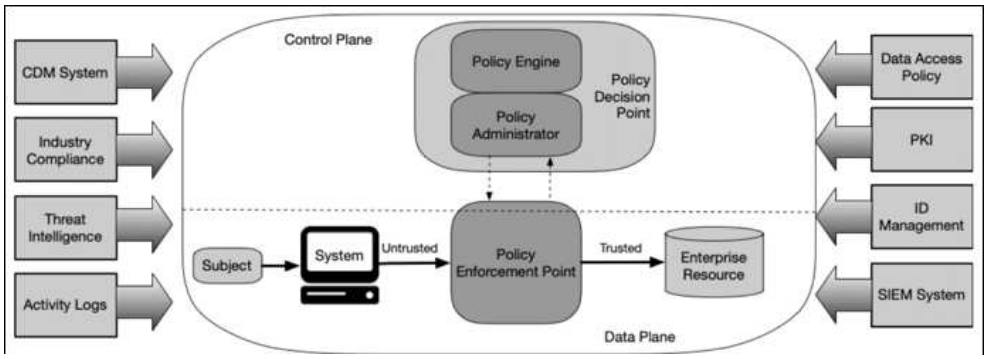

Figure 1:Core Zero Trust Logical Components, conceptual layout of Zero Trust Architecture (ZTA), adapted from NIST SP 800-207. The model separates the control and data planes, enforcing access policies through centralised decision points and continuous monitoring of users, systems, and data flows [23].

2.3 Threats and Vulnerabilities in Cloud Communications

Cloud communications services which include Voice Over Internet Protocol (VOIP), video conferencing, messaging etc and they are vulnerable to various cyber threats. According to the latest literatures data breach, insecure API’s, Denial of Service (DoS), lack of encryptions, poor Incident and Access Management (IAM) are some of them [12].

2.3.1 Data Breach

Data breaches are the one of the most critical concerns in this field occur from unauthorised access to data store in the cloud, where the consequences of these breaches vary based on the sensitive data which the user has handled. According to a study, the cause of data breaches is

increasing day by day because of certain factors which includes vulnerability due to shared resources where multiple organizations shares the same physical infrastructure which could lead to improper isolation controls, the other factor which the study projects that the organisations lose control over the data when stored in the cloud and have certain limitations which could lead to unauthorized access [13].

Data breaches have happened mainly due to phishing attacks targets certain users with a goal of gaining unauthorized access with the credentials. Phishing is considered as one of the most common tactics used by the attackers to gain control to the cloud environment, and due to the rapid increase in this attack introduction of Multifactor Authentication (MFA) has reduced the intensity of this attack up to certain extend [14].

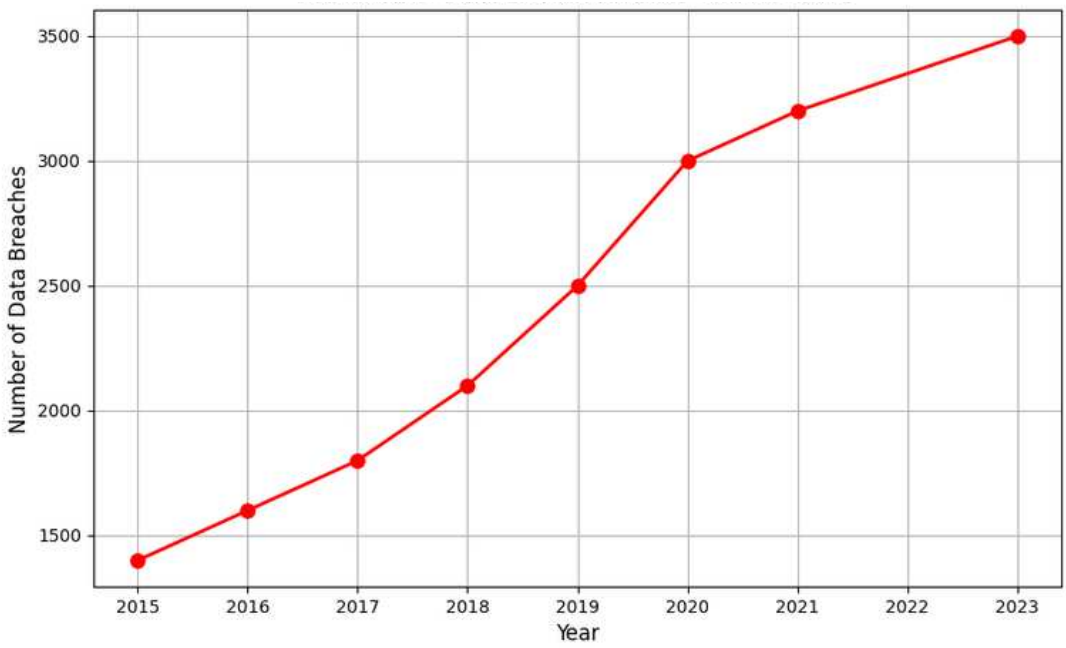

Figure 2: Increase in Data breach over the recent years. This chart illustrates the growing frequency of data breaches globally, driven by evolving cyber threats and vulnerabilities. Adapted from IBM Security (2024) and ENISA Threat Landscape Report (2023).

2.3.2 Insecure API's

Application Programming Interface (API's) are the considered to be an important for cloud functionality, one of the reasons for security vulnerabilities in the API's are because of unsecured API's that could lead to weak authentication, encryption or validation that could help hackers to exploit valuable data from the cloud. According to a study report by Tim Keary, 92% of organisation has faced API related security incident in the past one year [15].

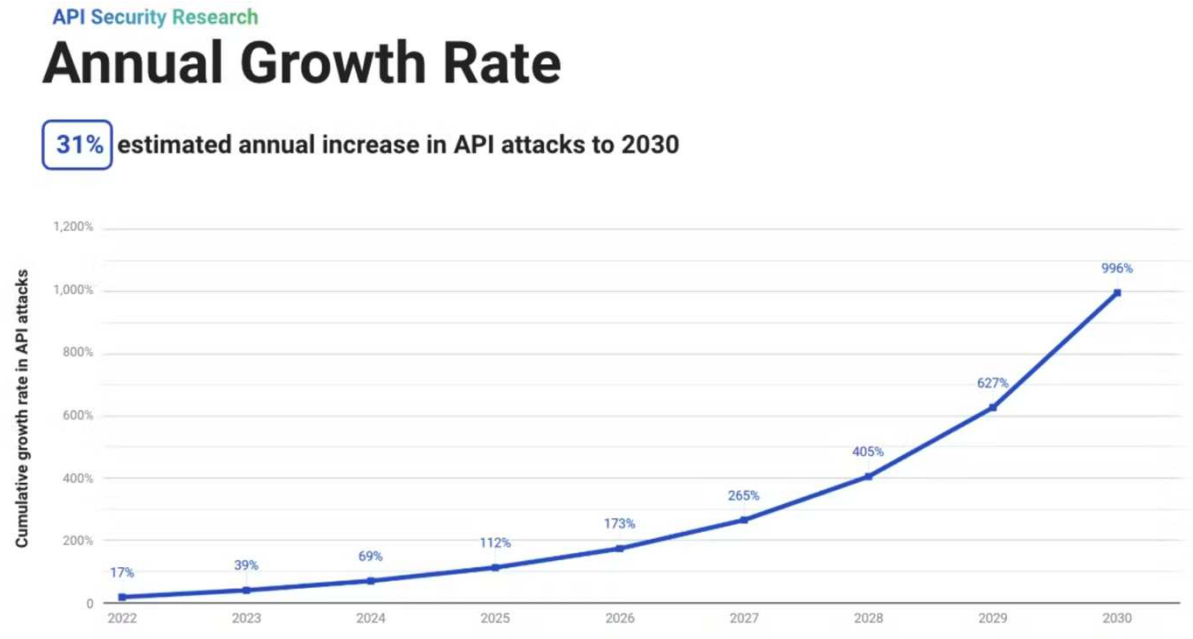

Figure 3: The Critical Role of APIs in Modern Enterprise Architecture. This diagram highlights how APIs enable integration, scalability, and resilience across cloud-based systems, including communication platforms [50].

2.3.3 Distributed Denial of Service (DDoS)

This attack, intend in overloading the cloud service making them unavailable for users, this attack could not to lead to deny of cloud services but also it can result in severe financial loss and reputational damage to the organizations. According to research by Khatoun and Zeadally [16], because cloud communication services' infrastructure has become dispersed, it makes them especially susceptible to DDoS attacks. According to their findings, the impact of DDoS assaults on cloud communication systems can be lessened by implementing sophisticated mitigation techniques including traffic filtering and rate-limiting algorithms.

According to the Cloudflare, they showcase that preventing DoS attacks can be challenging, particularly during high-traffic periods or across a vast and distributed network architecture. They are also recommending some prevention methods for DoS attacks which include attack surface reduction, anycast network diffusion, Realtime adaptive threat monitoring, caching and so on. Along with these preventions, they are also suggesting some tools which includes Web Application Firewall (WAF) which helps prevent attacks by filtering, inspecting, and blocking harmful HTTP traffic between web applications and the Internet using customisable policies, Secondly, Always on DDoS mitigation where a provider can help regularly examining network

traffic, adjusting policies in response to new attack trends, and maintaining a vast and dependable network of data centres [17].

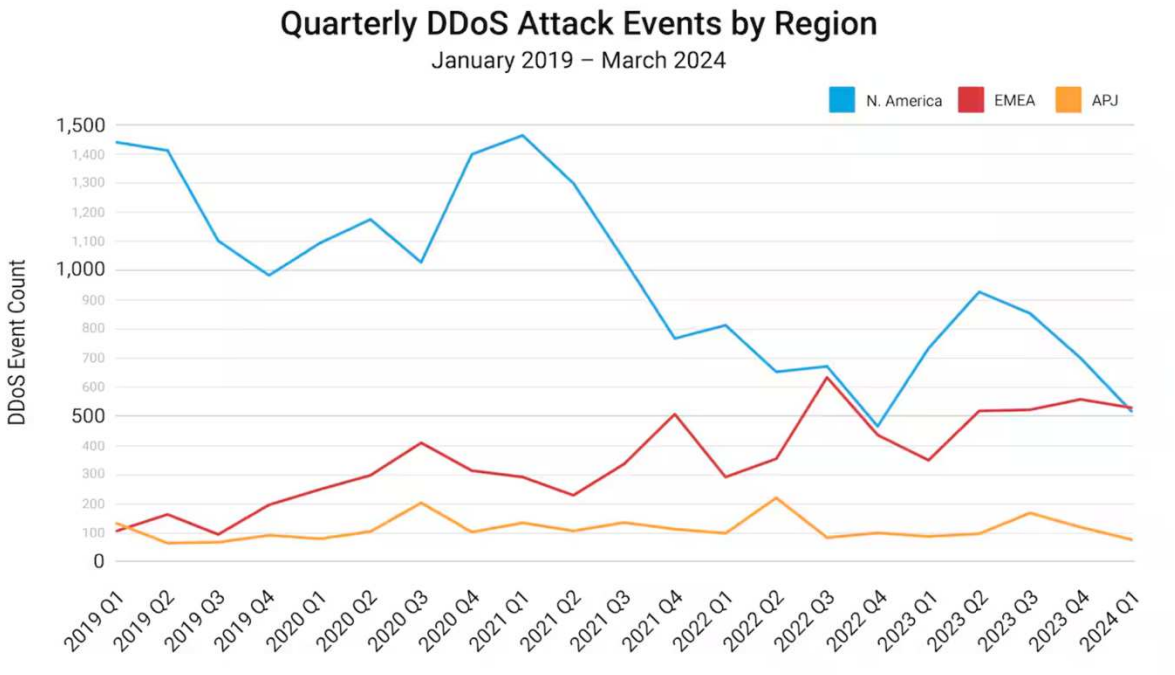

Figure 4 Rising Trend of DDoS Attacks in Europe, Middle East, and Africa region. This chart illustrates the sharp increase in DDoS attack frequency and intensity within the EMEA region, as reported by Akamai [51].

2.3.4 Lack of Encryption

Encryption is part of protecting sensitive data, which is stored in cloud, however information that doesn't have a strong encryption can easily be incepted and accessible by unauthorised people Businesses that fail to encrypt sensitive information expose it to breach risks and non-compliance with privacy regulations [12].

Failure to implement proper encryption practices often creates problems from oversight, inadequate policies, or misconfigured systems. For example, cloud environments may contain data in backup repositories or databases that are left unencrypted, inadvertently providing an easy target for attackers. Moreover, while many cloud service providers offer encryption capabilities, the shared responsibility model places the onus on businesses to ensure that their data is appropriately secured.

According to Scoop Market US (2024), encryption software adoption has steadily increased as organizations recognize the growing risks of data breaches and compliance requirements. The

report highlights that businesses are increasingly investing in encryption solutions to protect sensitive data both at rest and in transit [56].

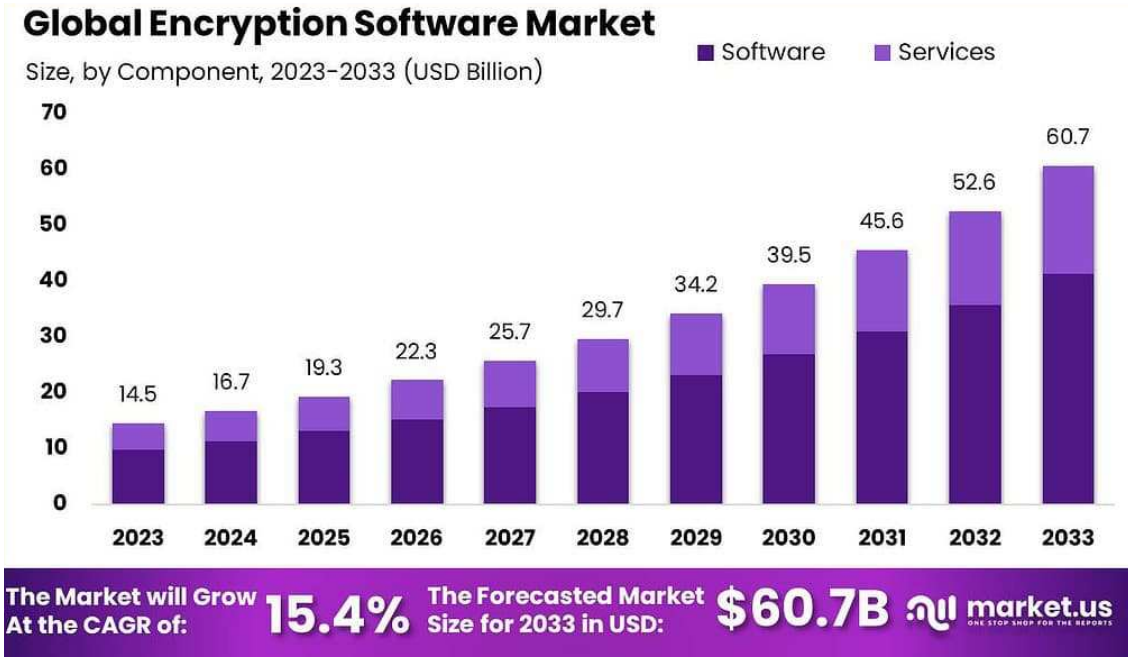

Figure 5: Projected Global Encryption Software Market Growth (2023–2033). This chart illustrates the rapid increase in market size for encryption software and services, driven by rising cybersecurity threats and regulatory compliance [56].

2.3.5 Poor Incident and Access Management (IAM)

Certain poor IAM practises such as weak password policies, giving too many permissions can expose cloud resources to unwanted access. Account hacks and data breaches are made possible by these IAM misconfigurations. To reduce the danger of unwanted access, IAM regulations and their corresponding MFA enforcement must also be reviewed on a frequent basis [12].

When access controls are weak or misconfigured, unauthorized users may gain entry to critical systems, potentially exposing sensitive data or disrupting operations. Additionally, organizations that lack proper incident detection and response capabilities may struggle to identify and contain security breaches, leading to prolonged exposure and greater damage [12].

Figure 6: Organizations confidence in the effectiveness of their Identity and Access Management program [57].

2.4 Famous Security Breaches

The cloud communication sector has witnessed several high-profile breaches that reveal systemic vulnerabilities:

2.4.1 Zoom (2020)

Over 500,000 Zoom accounts were compromised and sold on the dark web. The breach was attributed to credential stuffing, highlighting users' reliance on weak or reused passwords and Zoom's initial lack of multi-factor authentication (MFA). This incident pressured the company to introduce stronger encryption protocols and enhanced identity verification [14].

Because of this security breach, the company had multiple damages which includes, financial loss where, many organizations banned Zoom as a communications platform, resulting in direct lowered revenues for monthly subscriptions. Secondly, operational loss where increased time and effort taken to reset user details. Zoom instituted new security controls for meetings, including new password requirements. Thirdly, compliance where Impacts could include fines and liabilities such as breach disclosure notices or penalties levied by regulators and finally,

reputational loss where Zoom suffered negative publicity based on verbiage and visuals presented. [52]

2.4.2 Twilio (2022)

Twilio, a leading cloud communications platform, suffered a targeted phishing attack were attackers impersonated IT administrators. This social engineering campaign compromised employee credentials and granted access to sensitive customer data. The breach emphasized the importance of internal phishing awareness and the adoption of Zero Trust policies [14].

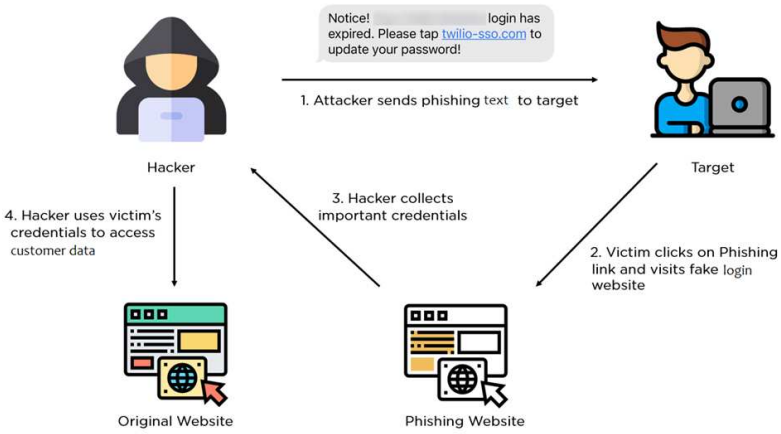

Figure 7: Visual Summary of the Twilio Smishing Attack (2022). This diagram illustrates the stages of the Twilio smishing attack, including phishing message delivery, credential harvesting, and unauthorized data access [53].

2.4.3 Microsoft Teams (2023)

A vulnerability related to the handling of GIFs in Teams allowed attackers to hijack user sessions without credentials. While quickly patched, the issue underlined the risks of improperly secured APIs and third-party integration points within real-time cloud communication systems.

These breaches demonstrate that even the most prominent providers are vulnerable if security is not continuously assessed and improved. Common attack vectors include weak access controls, misconfigured cloud storage, inadequate encryption practices, and phishing-based credential theft.

The **Cloud Security Alliance (CSA)** also lists the top threats to cloud computing in 2024, which includes:

- Insecure interfaces and APIs
- Misconfiguration of cloud services
- Lack of cloud security architecture and strategy
- Insider threats and human errors

As Sentinel One (2024) observes, these risks are compounded by the complex, shared-responsibility model in cloud environments where security responsibilities are split between providers and clients [12].

Furthermore, Verizon's Data Breach Investigations Report (2023) highlights that cloud assets are now the primary target in 80% of financially motivated cyberattacks [30]. This reflects the need for layered defences which include identity-centric access, anomaly detection, and regular security posture reviews.

2.5 Emerging Security Trends and Technologies

Advanced security measures are needed as the cloud systems continue to get complicated. To stay up with the changing threats that may help in exploiting vulnerabilities in the cloud infrastructure and the recent development in the cloud infrastructure which included the use of artificial intelligence (AI) and machine learning (ML), which are changing the way threats are found and dealt.

More and more organisations are using artificial intelligence (AI) and machine learning (ML) automate to find the unusual behaviour of systems and suspect violations. These systems can analyse massive databases, identify patterns of normal and abnormal conduct, and generate alerts or automatic responses to reduce dangers. According to McKinsey & Company [54], AI-driven threat detection systems can reduce the average time to detect security incidents by up to 60%, while reducing false positives, which can put stress on security staff. Whereas Blockchain technology has emerged as a promising solution for enhancing data integrity, transparency, and trust in cloud communication systems. Blockchain, with its decentralised and resistant ledger features, can provide immutable records of transactions, user interactions, and data updates.

2.5.1 Artificial Intelligence and Machine Learning

According to a study conducted by the Deloitte [18], Artificial intelligence and Machine learning are transforming in security which enables this system to detect and respond to threats. These systems scan large datasets to identify if there are any anomalies and predict if any chance of potential threats or if they have encountered any threats, it will activate the defence mechanism automatically.

According to Berman [19], AI systems can detect complex patterns and can defend itself against insider threats which traditional security measures often miss by the system, providing a robust defence against zero-day attacks and insider threats. Machine Learning (ML) algorithms can also be trained to detect the attacks and its existing patterns which also enables early identification of potential attacks, and this is done by collecting the vast historical data where machine learning algorithms are able to identify "normal" behaviour and highlight any differences that can indicate security risks and can continuously monitor , analyse data in real-time, warning security teams of potential risks before they materialise into full-fledged attacks, this capability is very beneficial for cybersecurity [20].

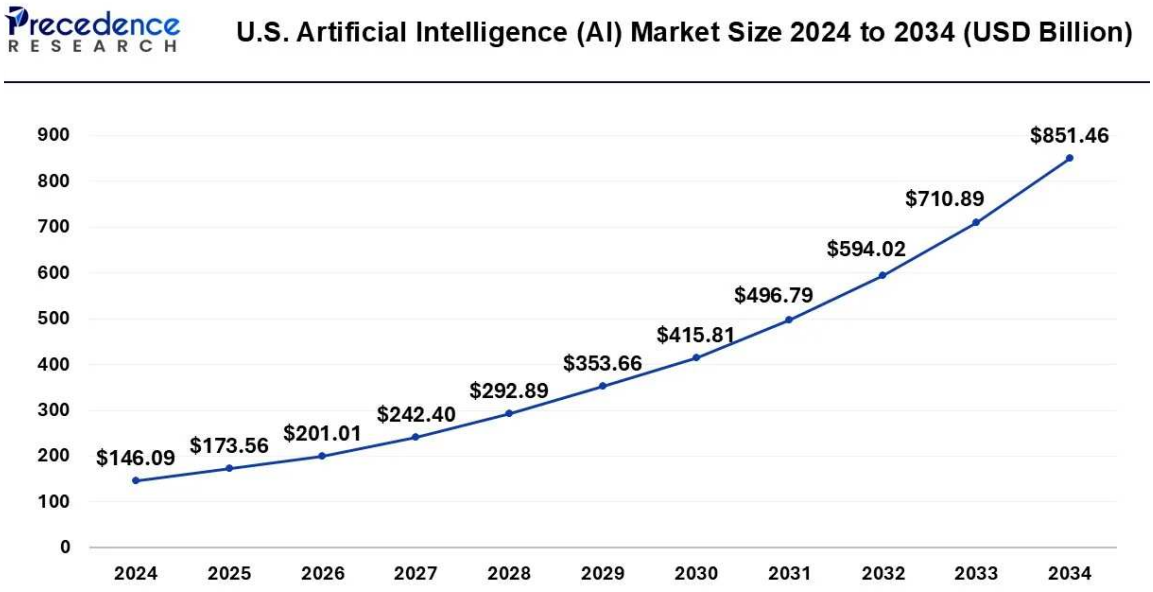

Figure 8 : Projected Growth of U.S. Artificial Intelligence Market (2024–2034).
This chart illustrates the steady and significant increase in AI market size, driven by advancements in machine learning, automation, and data driven decision making [55].

2.5.2 Block Chain Technology and its Integration

Block chain technology offers a decentralised approach for securing data integrity and managing identities, because of its decentralised approach blockchain is nearly indestructible to hackers manipulating the data on the network. Its immutable ledger structure ensures that information cannot be changed after it has been recorded, which is especially useful for preserving transparency and confirming the accuracy of communication data [21].

In addition, block chain can also identity management by securely storing user credentials in decentralised way which eliminates the need for centralized databases, which are often targets for hackers. To improve identity verification and safe access control in cloud communications, recent research has come up with the combination of blockchain technology and smart contracts where these strategies help in offering strong security and transparency by utilising the decentralised and unchangeable ledger of blockchain technology and the key developments are Decentralised Identity Verification (DIV), where a system that automate identity verification and certificate issuing through the use of blockchain-based smart contracts in Public Key Infrastructure (PKI) systems. The goal of this integration is to create a digital trust framework that is more user-centric, transparent, and safe [22]. This innovation not only strengthens authentication processes but also mitigates the risk of unauthorized access, which is a major concern in cloud environments.

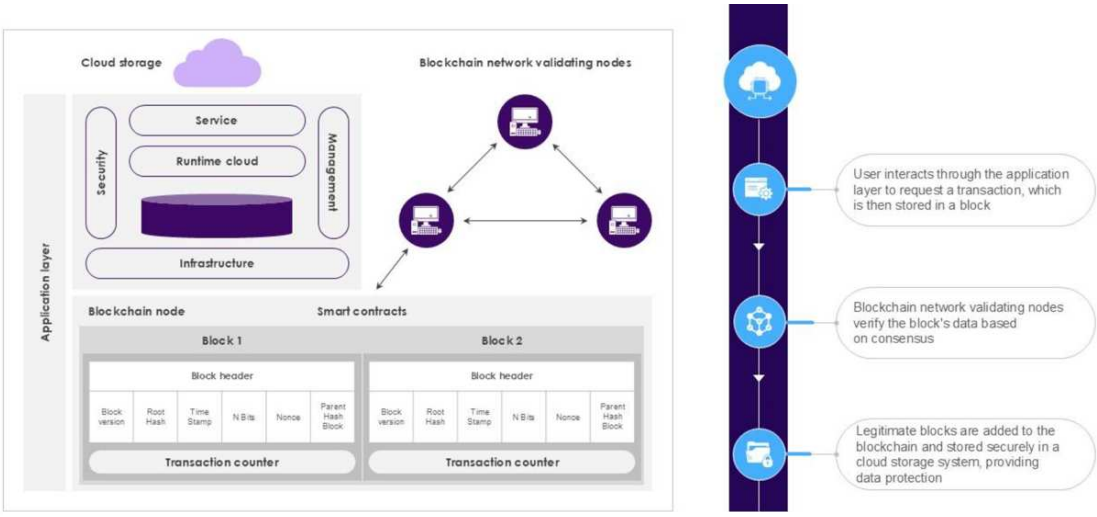

Figure 9: Blockchain-Integrated Cloud Architecture for Secure Transaction and Data Storage.
This diagram illustrates how user transactions pass through the application layer, are validated by blockchain nodes through consensus, and are securely stored within cloud infrastructure [58].

2.5.3 Zero Trust Architecture

Most companies have given up the original perimeter-based security paradigm in favour of zero trust architecture, which enforces strict access rules and verifies that every request originates from an untrusted source both inside and outside the network. Since data is continuously accessed from various devices and locations, exposing systems to increased risks of unauthorised access and insider threats, this model shift is crucial for cloud communication firms. One of the key principles ensure that the that devices and users only have the minimum amount of access needed to carry out their tasks, minimising the attack surface in the event of a breach. By demanding identity verification at every access point and frequently combining multi-factor authentication (MFA) with contextual data, like location or device type, to dynamically assess risk, continuous authentication further improves security [23].

If the cloud communication companies can adopt to Zero Trust Architecture, it offers many significant advantages whereby continuous verification and zero trust improve compliance with regulatory requirements like General Data Protection and Regulation (GDPR), which require strict data access restrictions, and lower the risk of data breaches. Additionally, zero trust improves network activity visibility. Administrators can have up-to-date insights into user behaviour because each request must be verified, which makes it simpler to identify irregularities that could point to a security breach [24].

While implementing this Zero trust architecture is highly beneficial for the systems, implementing it with platforms is certain challenging. One major obstacle is the need for extensive integration with existing infrastructure, which may require substantial modifications to legacy systems, and it is also costly as well.

2.5.4 Identity and Access Management

Identity and access management (IAM) plays a major role in cloud security which ensures that the right individuals are given the access, at the right time on the right resource. IAM helps cloud communication systems keep track of user identities and implement security regulations in many places at once. Many businesses are facing multiple issues while implementing IAM methods which are successful, and the reason for certain unsuccessful IAM methods include poor user provisioning, not proper access reviews and inconsistent enforcement of least privilege principles.

According to the recent study conducted by the European Journal of Engineering and Technology Research group (EJETR), IAM is no longer considered as a minor component of IT. Instead, it plays an integral part in making organisations safer and more efficient. The study points out that common vulnerabilities used in cloud communication breaches include poor access control, delayed deprovisioning of former personnel, and a lack of periodic access audits and the findings also preserves the importance of implementing identity life cycle management and using of automation techniques to reduce human error.[59].

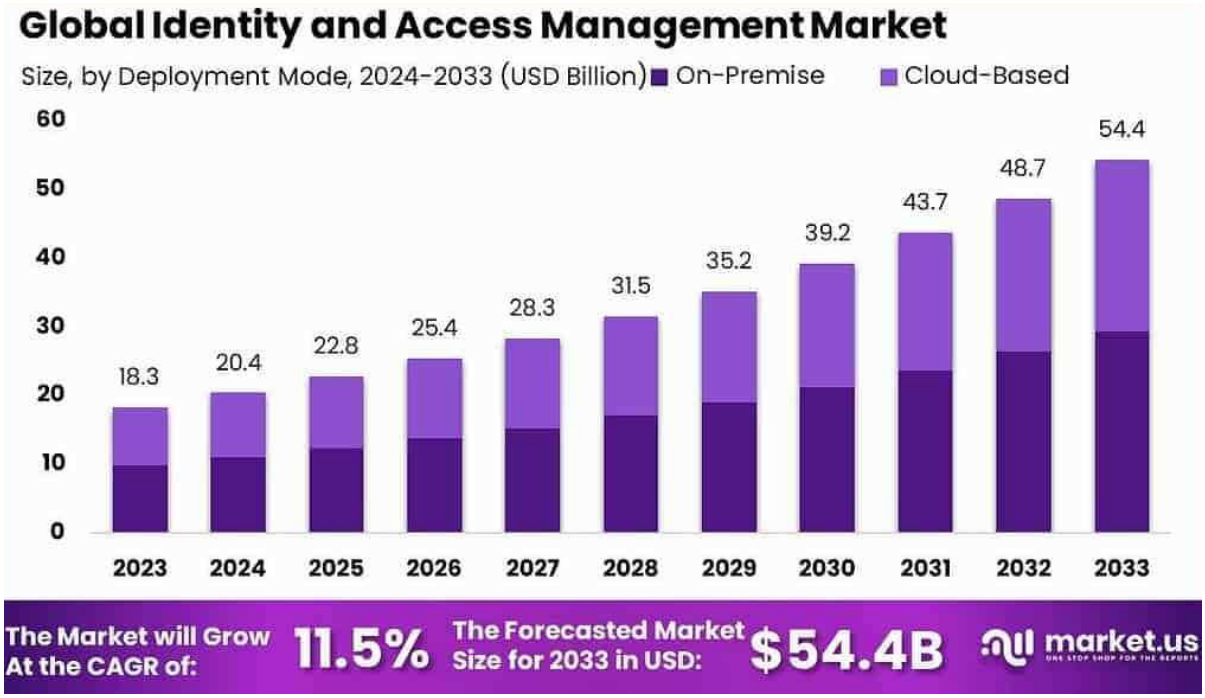

Figure 10: Projected Growth of the Identity and Access Management Market (2023–2033).

This chart illustrates the market expansion of IAM solutions, showing growth in both on-premises and cloud-based deployments, driven by rising cybersecurity and compliance demands [60].

According to this chart, the global Identity and Access Management (IAM) market is expected to develop steadily, reaching $54.4 billion by 2033. And this future growth can lead to demand in identity controls within the organisations and majority of the organisations primary focus will be on implementing high secured identity controls to prevent data breaches, ensuring regulatory compliance, and supporting remote work environments.

To summarise, identity and access management is developing into an integrated security discipline that integrates protection, user experience, and compliance. As cloud infrastructure increases, safeguarding those cloud infrastructure is also needed.

2.6 Existing Research on Cloud Communication Security

Academic work has increasingly focused on securing cloud communication channels. Shanmugam (2016) proposed enhancements to SRTP and DTLS for improving the confidentiality of cloud conferencing platforms [4]. Berman et al. (2019) presented the role of deep learning in detecting malicious user behaviour patterns, particularly in real-time messaging systems [19].

A recent study by Alshahrani and Simpson (2023) evaluated the impact of MFA on reducing account compromise incidents in cloud environments, demonstrating a reduction in successful phishing attempts by up to 60% [14].

Despite these advancements, there remains limited research on small to medium sized communication service providers and how emerging technologies such as AI/ML and blockchain can be pragmatically applied to their infrastructure.

2.7 Gaps in the Literature

While significant progress has been made in developing security frameworks and technologies for large cloud service providers, literature remains sparse on tailored solutions for mid-sized providers like Moitele. Most frameworks assume enterprise scale resources, overlooking implementation challenges such as cost, integration complexity, and workforce limitations.

This thesis addresses that gap by using Moitele as a case study to derive a security strategy that is practical, scalable, and resource aware.

3 Methodology

3.1 Introduction

This chapter gives the outline about the specific research methods used to investigate the security practises and challenges the company have faced during its operations. The company's name is Moitele, a telecommunication service provider located in Turku, Finland. This research employs a case study methodology by concentrating on a single organisation, which enables a comprehensive analysis of actual security challenges encountered in a particular company's operations and provide them insights into real-world security measures and offers recommendations as per the company's need.

3.2 Research Design

3.2.1 Case study approach

The case study approach was chosen for this thesis is because, it helps to focus on a specific company and do an analysis for the same. Case studies are the most effective for exploring complex issues in real life and provide a comprehensive view for the same. By this approach provide the understand of the security practises and specific challenges company has faced which helped suitable for doing my work in the relevant field.

This case study approach has helped in understanding more about the company's security practices and some certain questions which include whether the company has encountered any security challenges, or have they implemented the latest emerging technologies which include Zero Trust Architecture (ZTA) or AI driven detection systems which I have already explained in detail in the previous chapter.

3.2.2 Mixed method strategy

A mixed method strategy combining quantitative and qualitative data was originally planned [25][26]. The goal was to complement the numerical insights from a survey with deeper, contextual information gathered through interviews. However, due to constraints during data collection including a low response rate for the survey and the completion of only one interview the full implementation of this mixed-method approach was not feasible.

3.3 Data Collection

3.3.1 Quantitative Component

A structured survey with 20 questions was prepared and distributed via Google Forms to Moitele employees, covering topics such as security practices, perceived threats, awareness of emerging technologies, and general background information. The response rates from the users weren't sufficient for the meaningful analysis, so because of that no formal quantitative findings are presented, the available responses are recognised in a limited descriptive manner without statistical analysis.

3.3.2 Qualitative Component

A formal interview was conducted with the CEO of Moitele, focusing on the topics such as current security practices, recent challenges, and future strategies. The original or initial plan was to conduct multiple interviews with company's board members and other co employees and perform the thematic analysis using NVivo software. However, due to limited participation, only one interview was completed. So, instead of thematic analysis, the findings from this interview are presented in a straightforward question-and-answer (Q&A) format in the results section.

3.4 Data Analysis

This section describes the approach initially planned for analysing the data collected in this study. The original research design idea was to use a mixed method analysis, a combination of statistical methods for survey answers combined with thematic analysis of data from qualitative interviews. However, due to the limited number of participants and the completion of only one interview, the analysis approach was modified to fit the available data. Quantitative findings are also limited to descriptive observations, and qualitative insights are presented in a straightforward Q&A format based on the CEO's responses.

3.4.1 Quantitative Data Analysis

The initial proposed plan was to analyse survey data (from the google form) using SPSS (Statistical Package for the Social Sciences), which performs descriptive and predictive statistical analyses [27][28]. However, due to limited number of responses, meaningful analysis could not be performed.

3.4.2 Qualitative Data Analysis

Thematic analysis using NVivo was originally planned initially to get themes and patterns from multiple interviews [29][32]. However, due to the limited number f of only one interview, thematic analysis was not feasible. Instead, the findings from the CEO interview are presented as a raw Q&A format in Chapter 4, representing the CEO's direct responses without interpretation or coding.

3.4.1 Justification for Software Selection

SPSS and NVivo were initially chosen because of their great ability to handle quantitative and qualitative data [27][29]. However, due to the restricted amount of data obtained, these techniques were not used for analysis, and descriptive presentation methods were used instead.

4 Findings

4.1 Introduction

This chapter presents the results of the study, which illustrates the planned mixed-method approach. However, due to limited participation in both the survey and interview, the findings are presented in a descriptive form. The quantitative data i.e. survey data is summarized, while the qualitative insights from the CEO interview are presented in a question and answer (Q&A) format.

As a whole, these findings offer valuable insights into Moitele's security posture and form the foundation for the proposed security framework in Chapter 5.

4.2 Survey

While the survey was designed to explore employee perspectives on key elements of Moitele's security framework including Zero Trust Architecture (ZTA), AI/ML adoption, incident response, and may other as well, but only two participants responded. As a result, these findings are presented as observations rather than representative conclusions. They provide insights into the viewpoints of the respondents and highlight potential areas for further exploration in future research.

- Role Based Access Controls (RBAC)**:** Although one person expressed uncertainty about the effectiveness of RBAC's current implementation, all participants agreed that it could improve access control.

- Understanding of Zero Trust Architecture (ZTA)**:** Both respondents admitted that they were unsure of the specifics of ZTA's implementation, they were at least somewhat familiar with the idea. They indicated that they would be interested in finding out more about how it may improve Moitele's security.

- Use of Multi Factor Authentication (MFA)**:** Both respondents noted that MFA is actively used in their daily processes, and they feel that it provides a solid layer of security for accessing systems.

- Continuous Monitoring and Anomaly Detection: Both participants agreed that whether such systems are in existence at Moitele now, but both agreed that it would be useful to have systems in place to continuously monitor for anomalous activities.

- Automated Security Alerts and Responses: Both respondents viewed automated security responses as a positive, particularly for reducing response times during incidents. But they also highlighted on how crucial is to maintain human monitoring.
- Use of AI for Security: Both participants reported awareness of existing AI-driven security tools within Moitele. However, they both believed that advantages of AI for early threat detection and response could be beneficial for the organisation.
- Incident Response Preparedness: Both the participants felt they had a basic understanding of incident response procedures but also admitted that they would feel more confident with additional training.
- Automated Security Alerts and Responses**:** Both respondents viewed automated security responses as a positive addon, particularly for reducing response times during incidents. However, they pointed out the importance of maintaining human oversight.
- Security Awareness Training: One participant mentioned that while some basic security training has been provided, whereas the other didn't.
- Awareness of Blockchain for Security: Both of participant was aware and familiar with the use of blockchain technology for securing data integrity. However, they were ready and open to learning more if it were introduced.
- AI for Phishing Detection**:** Both the participants agreed that AI-based tools could be a helpful addition to identify and block phishing attempts, especially as attacks become more sophisticated.
- Blockchain for Log Integrity: Both participants felt this technological concept could add transparency and reliability but required further investigation.
- Communication of Emerging Security Trends: Both participants told that while some information is shared, more regular updates on emerging security technologies would be helpful.
- Real Time Monitoring and Alert Systems: Both the participants felt that real-time monitoring with proactive alerts would provide greater reassurance, but they have much knowledge about the current capabilities at Moitele.

- Role Specific Training: According to both participants, security training that is personalised for various positions inside the organisation will increase the relevance and effect of the material.

- Centralized Logging and Automated Detection: Both the participants expressed their interest in centralized logging systems with automated detection features. They felt that such systems could provide more comprehensive visibility into potential threats.

- Confidence in Backup and Recovery: While both participants felt that backup and recovery systems are in place.

- Clarity on Reporting Procedures: While both participants knew that security incidents should be reported, they were clear about the exact reporting steps and clearer communication.

4.3 Observations

The survey, though limited to two respondents, provided valuable observations that adhere to the strategic framework this thesis suggests. Both participants acknowledged the importance of foundational security measures such as Multi Factor Authentication (MFA) and encryption, which are the current strengths within Moitele's security posture. Both participants also highlighted significant gaps that directly correspond to areas which the company would like to improve in the proposed framework. Also, there was limited awareness of Zero Trust Architecture (ZTA).

Secondly, both the participants showed minimal familiarity with AI and machine learning-based security solutions, highlighting the need for Moitele to explore and integrate AI/ML technologies for proactive threat detection and incident response. The lack of awareness around blockchain technologies for data integrity and secure logging.

Thirdly, the survey responses pointed to a need for enhanced employee training and awareness, particularly in recognizing phishing attempts and responding effectively to incidents. This finding backs up the framework's focus on continuous learning, simulated phishing tactics, and interactive training sessions.

To conclude, although limited in scope, the survey observations reinforce the relevance and necessity of the proposed framework.

4.4 Interview

The following section presents the information obtained from a one-on-one interview with Moitele's CEO. The questions were designed to understand the company's current security practices, challenges, and future, particularly in relation to the points and recommendations in the proposed security framework. The answers are presented in a straightforward, descriptive manner to maintain clarity and transparency.

1. How would you describe Moitele's current security posture?

   Answer: Our security foundation is quite strong, with multi-factor authentication and encryption well established. However, we understand there's always a place for improvements as new threats emerge.

2. What are the main security challenges your company has encountered recently?

   Answer: We've had to deal with a brute force attack, but it was handled perfectly but still we feel we should strengthen our defences and review on a frequently.

3. What measures were taken following the brute force attack?

   Answer: We quickly contained the threat, reviewed our access controls, and reinforced our monitoring systems to prevent similar incidents.

4. Is Zero Trust Architecture (ZTA) currently implemented at Moitele?

   Answer: No, we haven't implemented ZTA yet. It's a recent approach we're aware of, but it hasn't been adopted at this stage.

5. Are there plans to explore ZTA in the future?

   Answer: It's something we're not considering now, but we feel it requires careful planning and resources. Right now, we're focused on maintaining our current systems.

6. Does Moitele use AI or machine learning for security purposes?

   Answer: Not now. We haven't integrated these technologies into our security framework.

7. What are the key security technologies used in the company today?

   Answer: I can't give a detail information, but all I can say that rely on strong encryption, multi factor authentication and few other security measures which are confidential.

8. Is there a formal incident response plan in place?

   Answer: Yes, and we review them periodically.

9. How does Moitele manage employee awareness around security?

   Answer: We provide basic training, and we believe it's always self-learning.

10. Have you conducted simulated security incident drills?

    Answer: No.

11. Are there clear protocols for employees to report suspicious activity?

    Answer: We have reporting channels in place.

12. How is data encryption handled across systems?

    Answer: All sensitive data is encrypted during transmission, and we're committed to maintaining encryption standards.

13. Have blockchain technologies been considered for data integrity?

    Answer: No, not in the plan as of now.

14. How confident are you in your backup and recovery processes?

    Answer: We are confident.

15. Is role-based access control (RBAC) applied across systems?

    Answer: Yes, RBAC is implemented.

16. Do you believe that adopting micro-segmentation could improve security?

    Answer: I have heard about that concept, but I believe that could help contain potential breaches, but it's not something we've implemented.

17. Do you feel Moitele's security practices are evolving fast enough to keep up with emerging threats?

    Answer: We try our best, but there's always more to be done. Security is an ongoing effort, and it's something we're committed to improving.

18. Is Moitele considering automated security responses for incidents?

    Answer: Not in our plans currently, but I believe human oversight remains crucial even though we have automated security responses.

19. Are employees required to use VPN when working remotely?

    Answer: No, it's not mandatory.

20. How are security patches and updates handled?

    Answer: Critical patches are applied promptly on regular scheduled updates.

21. Do you conduct regular security audits or assessments?
    Answer: Yes, we have internal reviews to check compliance and identify potential vulnerabilities.

22. Are there plans to integrate AI/ML-based anomaly detection?
    Answer: It's a possibility we're exploring, but it will require the right tools and expertise to implement effectively.

23. How do you approach employee education on new security threats?

    Answer: Like I said, we don't educate them on a regular basis, we just provide them the basic training and rest is self-learning.

24. Do you think more resources should be allocated to security?

    Answer: Definitely.

25. Is there a dedicated team responsible for security?

    Answer: Yes, we do have a team.

26. Would you support more investment in advanced security solutions?
    Answer: Yes, if needed, investing in modern security tools and frameworks is essential for keeping our systems, data safe and built trust with our clients.

27. What's your view on the future of security at Moitele?
    Answer: We're aiming for a more proactive approach, incorporating new technologies and improving training to stay ahead of evolving threats.

4.5 Observations

The findings gathered from the CEO interview, while limited to a single perspective, emphasis on maintaining strong foundational practices such as multi-factor authentication and encryption shows the existing security strengths identified in the framework. However, the interview also highlighted key gaps including the lack of adoption of Zero Trust Architecture (ZTA), minimal integration of AI/ML technologies, and limited preparedness for incident response.

The CEO's also is ready to explore blockchain for data integrity and automated security responses further supports some framework recommendations for adopting innovative technologies. Additionally, the recognition of a need for better employee training, role specific education, and simulated security drills are needed.

5 Proposed Security Framework

5.1 Introduction

Because cloud services are distributed, cloud communication enterprises are increasingly vulnerable to cyberattacks. Based on the findings from the survey and interview findings, this chapter proposes a comprehensive security framework tailored specifically for enhancing the security posture of Moitele. The proposed framework shows key recommendations from both conceptual frameworks and real world security tactics identified during this research.

The newly proposed method takes a multi-layered approach, including safegurading, investigate, and defensive security measures to reduce risks and vulnerabilities connected with Zero Trust Architecture (ZTA), AI/ML security gaps, and encryption practices. This holistic security approach is designed to respond to the changing security environment while ensuring data protection and business continuity.

5.2 High Level Architecture Overview

The proposed architecture consists of five core layers: Identity & Access Management Layer, Access Control and Zero Trust Layer, Threat Detection & Intelligence Layer, Data Security Layer, and Monitoring and Incident Response Layer. These components work together to encrypt communication, control access, detect anomalies, and ensure data integrity.

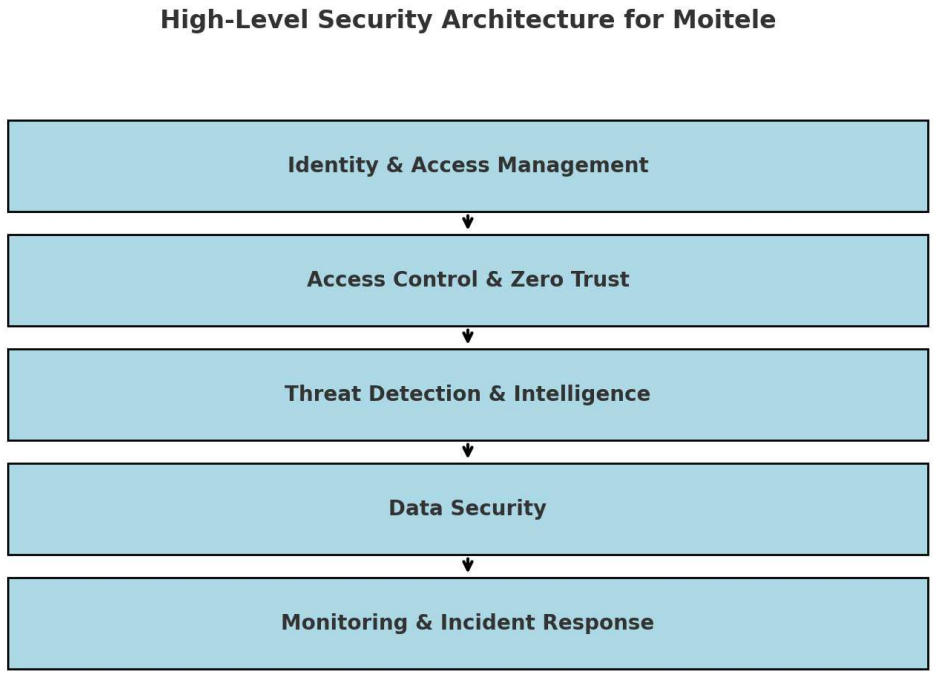

Figure 11: Technical architecture layers of the proposed security framework.

5.3 Key Components of the Security Framework

The new proposed framework for Moitele comprises five layers that together strengthen Moitele's security posture and these include:

- Zero Trust Architecture (ZTA): Establishing a "never trust, always verify" approach with strict identity-based security controls.
- Enhanced Incident Response: Improving detection, containment, and recovery protocols for faster threat mitigation.
- AI/ML Integration: Leveraging artificial intelligence for anomaly detection and proactive threat mitigation.
- Employee Awareness and Training: Cultivating a security-conscious workforce to mitigate risks from insider threats.

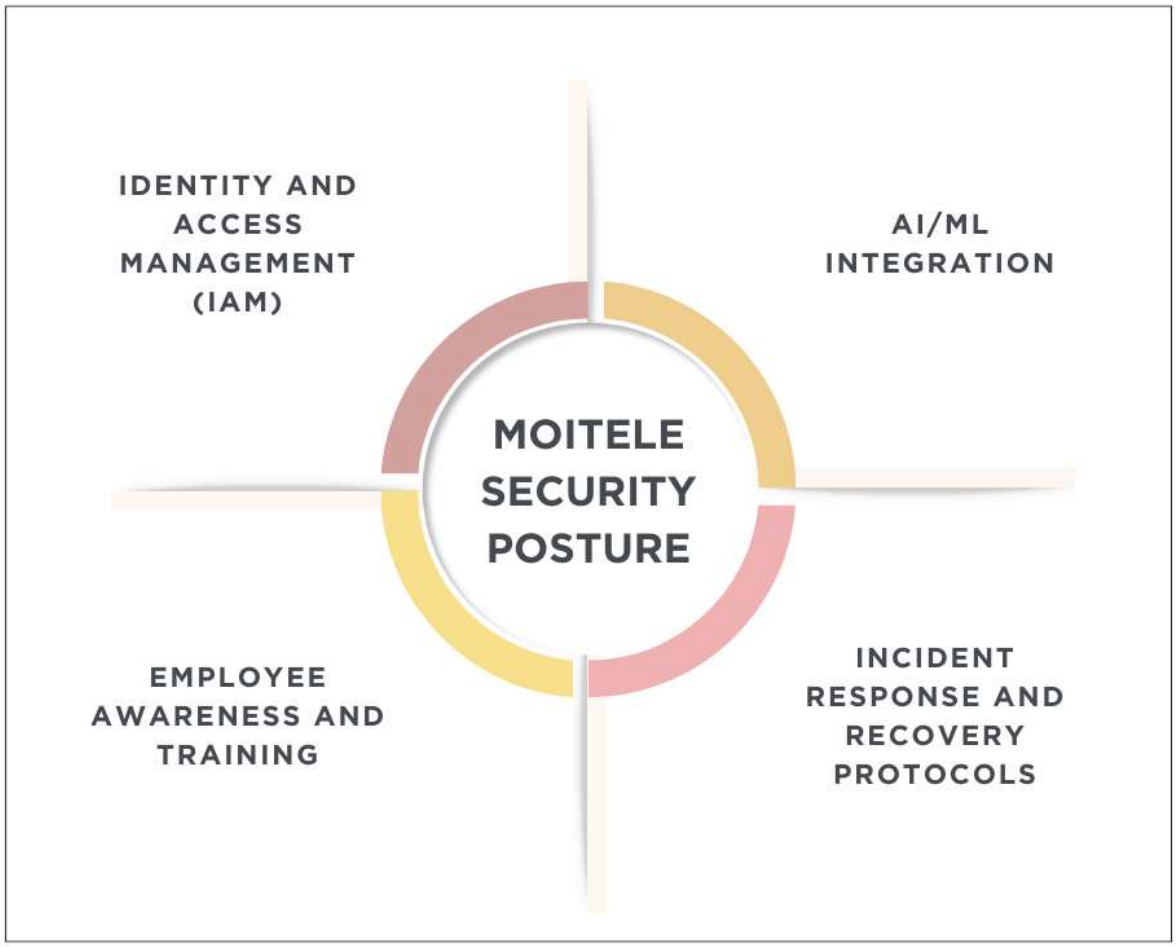

Figure 12: Proposed Security posture for Moitele

5.4 Detailed Explanations of Framework Components

5.4.1 Zero Trust Architecture

It is shown that Moitele has very minimal has minimal awareness and implementation of Zero Trust Architecture, this framework suggests adopting ZTA principles to mitigate potential vulnerabilities as it emphasises on “never trust, always verify” approach, ensuring that access to systems is continuously authenticated and monitored, implementing least privilege access controls will limit user permissions to only what is necessary for their roles. Given that Moitele has existing security strengths in MFA and encryption, ZTA will further boost their security by minimizing trust assumptions within networks.

5.4.1.1 Proposed Visual Representation of Zero Trust Architecture (ZTA)

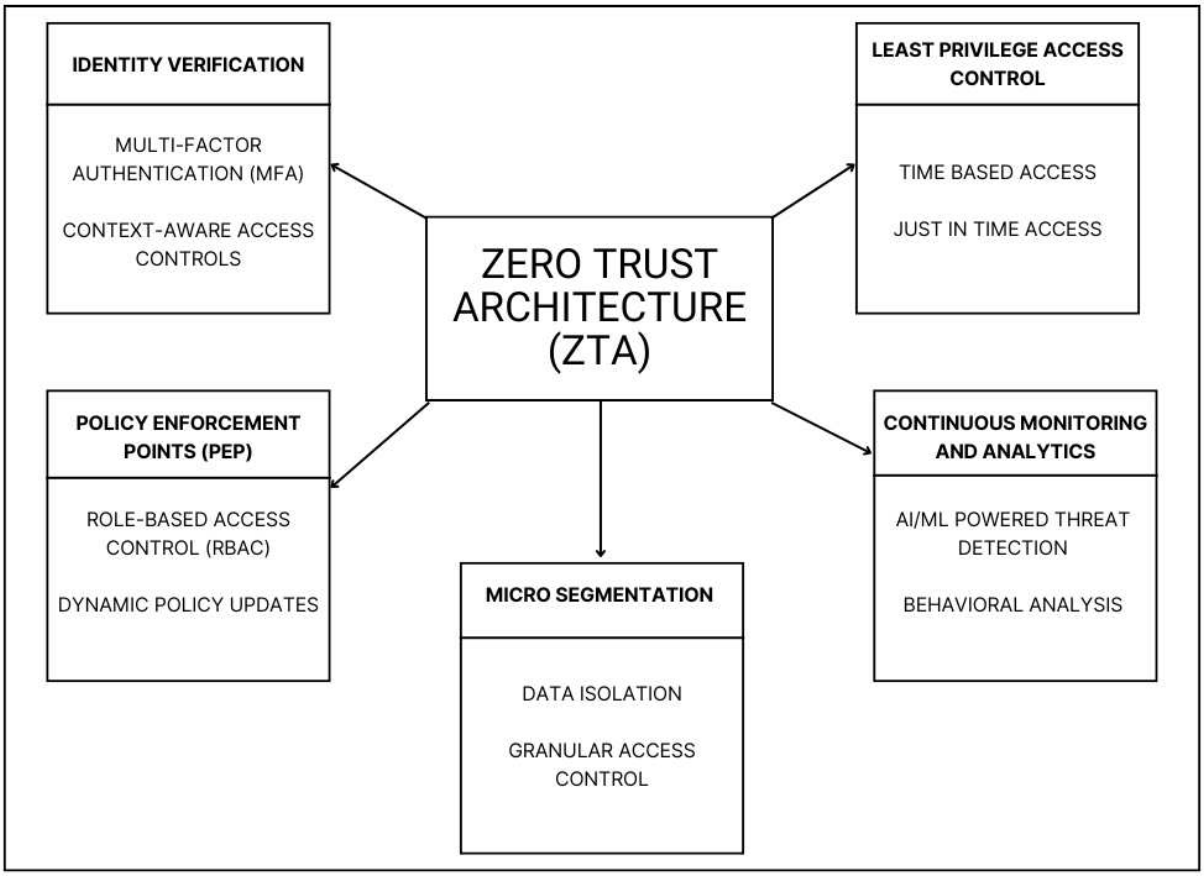

Figure 13: Visual representation of the proposed ZTA for Moitele's security infrastructure

5.4.1.2 Explanation of Framework Layers

- Identity Verification

  Zero Trust Architecture emphasizes identity centric security as a fundamental principle, ensuring that users are verified at every stage of network access [31], and identity

verification is the most crucial entry point in ZTA model, where every access request whether from employees, vendors, or remote users is verified before being granted.

- Multi-Factor Authentication (MFA)

  Moitele's MFA implementation has already secured user access. On top of this strong foundation, the ZTA model reinforces identity verification by introducing continuous session monitoring for identity anomalies.

- Context Aware Access Controls

  Access privileges will be constantly modified according to user behaviour, device health, and location.

o Least Privilege Access Control

Least privilege models have proven effective in minimizing security risks by ensuring that users only access what they need [32], Moitele can lessen the risk of insider threats or compromised accounts by limiting user rights to only what is required for their function.

- Time Based Access: Temporary access tokens are issued for critical system modifications, automatically terminated after use.

- Just in Time Access: Employees are granted access only when specifically required, reducing continues access privileges.

o Micro Segmentation

In the case of a breach, through the creation of separate network zones for essential business resources, micro segmentation lowers lateral mobility. Research highlights micro segmentation as a key strategy for mitigating lateral movement during attacks [33].

- Data Isolation: By seperating customer data, VoIP infrastructure, and internal resources, Moitele can limit potential attack vectors.

- Granular Access Control: Each segment has its own unique access policies, reducing exposure from internal threats.

- Continues Monitoring and Analysis

  Continuous monitoring enables proactive threat detection and incident response

  - AI/ML Powered Threat Detection: AI driven solutions can identify anomalies, unauthorized behaviors, and emerging threats.
  - Behavioral Analysis: By analyzing patterns, the system can detect deviations in user behavior and enforce automated security actions.

- Policy Enforcement Points (PEP)

  PEP is a core ZTA component that ensures security policies are strictly enforced during data exchanges, communications, or system interactions.

  - Dynamic Policy Updates: Policies are automatically adjusted based on risk assessment, ensuring that compromised endpoints or suspicious user behaviour is blocked immediately.
  - Role-Based Access Control (RBAC): Users are granted the minimum level of access required to perform their roles.

5.4.2 AI/ML in Security

Moitele hasn't adopted AI/ML technologies into the company's security framework, and this omission may lead to an attack, and by integrating AI/ML technology could increase valuable opportunity to enhance threat detection, automate incident response, and improve proactive defence mechanisms, and day by day AI/ML technologies have constantly upgrading security by enabling intelligent data analysis, anomaly detection, and behaviour prediction, making them increasingly essential in modern security strategies.

5.4.2.1 Proposed Visual Representation of AI/ML in Security

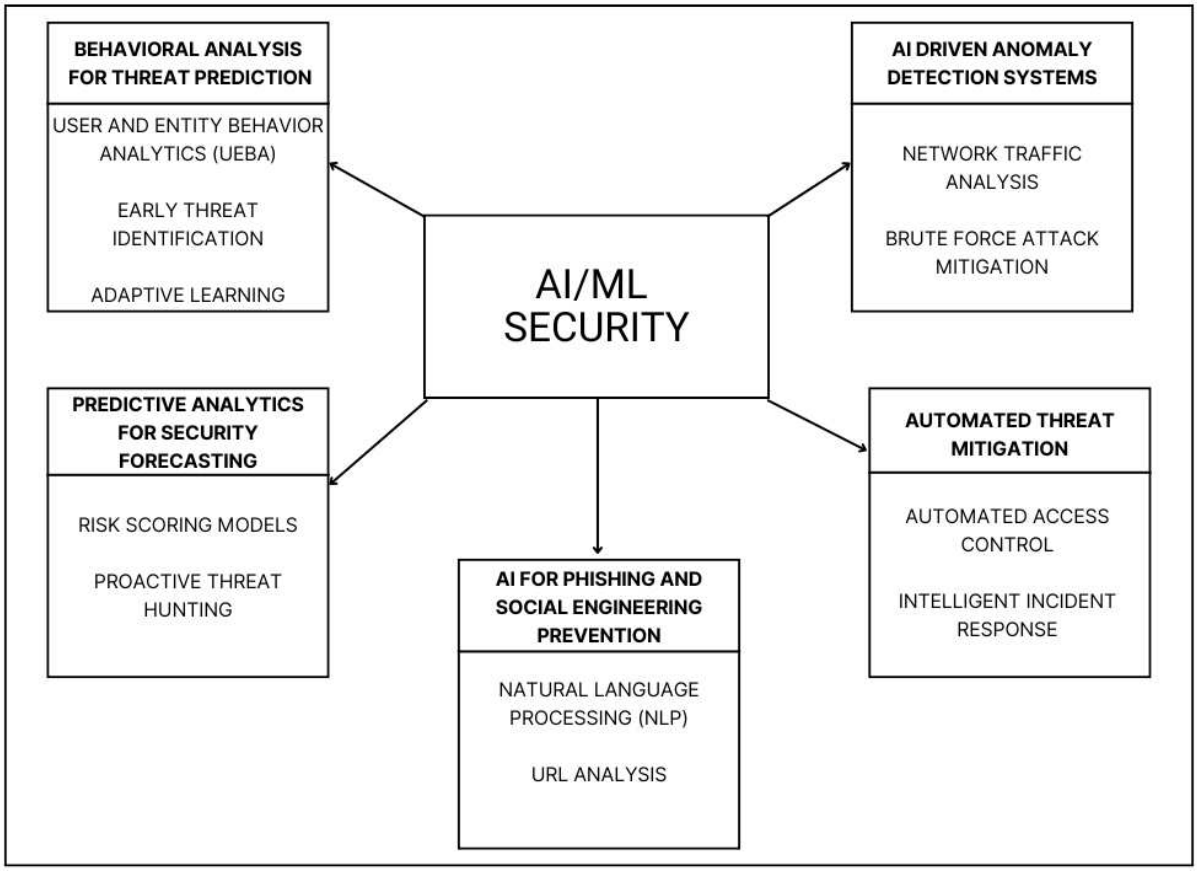

Figure 14: Visual Representation of AI/ML for Moitele in its current Security Infrastructure

5.4.2.2 Explanation of framework layers

- Behavioural Analysis for Threat Predictions

  Behavioural analysis utilizes AI algorithms to study user behaviour, identify deviations, and detect suspicious activities.

  - User and Entity Behaviour Analytics (UEBA): AI identifies deviations in user behaviour, which helps detect insider threats or compromised accounts.
    For example: login times, device usage, and access requests.

  - Early Threat Identification: For instance, if an employee suddenly downloads large volumes of customer data outside working hours, the AI system can flag this as suspicious activity.

  - Adaptive Learning: AI models continuously refine their understanding of behaviour, reducing false positives and improving threat prediction accuracy.

- AI Driven Anomaly Detection Systems

  Anomaly detection algorithms enable active identification of unusual patterns in data traffic, system performance, and user activity if it comes across.

  - Network Traffic Analysis: AI can analyse data flows to detect suspicious patterns such as Distributed Denial-of-Service (DDoS) attacks, command and control communications, or unexpected data exfiltration attempts.
  - Brute Force Attack Mitigation: With the Moitele's recent experience with brute force attacks, integrating AI based detection systems can enhance real time alerting and response capabilities.

- Automated Threat Mitigation

  AI systems can autonomously respond to security incidents by triggering predefined security actions.

  - Intelligent Incident Response: AI models can prioritize alerts, identify false positives, and suggest mitigation actions to their organisation security teams.
  - Automated Access Control: If a suspicious login attempt is identified, the system can automatically revoke access or require additional authentication layers.

- Predictive Analytics for Security Forecasting

  Using historical data, predictive analytics foresees security issues before they become real.

  - Risk Scoring Models: AI-powered risk assessment tools prioritise security threats by giving endpoints, user accounts, and apps security scores.
  - Proactive Threat Hunting: Security teams may concentrate on high-risk vulnerabilities before they are exploited through predictive solutions.

- AI for Phishing and Social Engineering Prevention

  AI models can analyse email content, message patterns, and metadata to detect and block phishing attempts before they reach employees.

  - URL Analysis: By checking online links for dangerous activity, AI systems can stop users from visiting phishing websites.

- Natural Language Processing (NLP): NLP algorithms can analyse email content, spot phishing signs, and mark potentially dangerous messages.

5.4.3 Incident Response and Recovery Protocols

Reducing the effects of attacks and guaranteeing quick recovery depend on good incident response systems. When it comes to Moitele, he proposed framework emphasizes strengthening their existing measures by adopting structured incident response and recovery protocols. For Moitele, recent experience with a brute force attack, enhancing their preparedness is crucial to minimize downtime, data loss, and potential reputational damage.

5.4.3.1 Proposed Visual Representation of Incident Response and Recovery

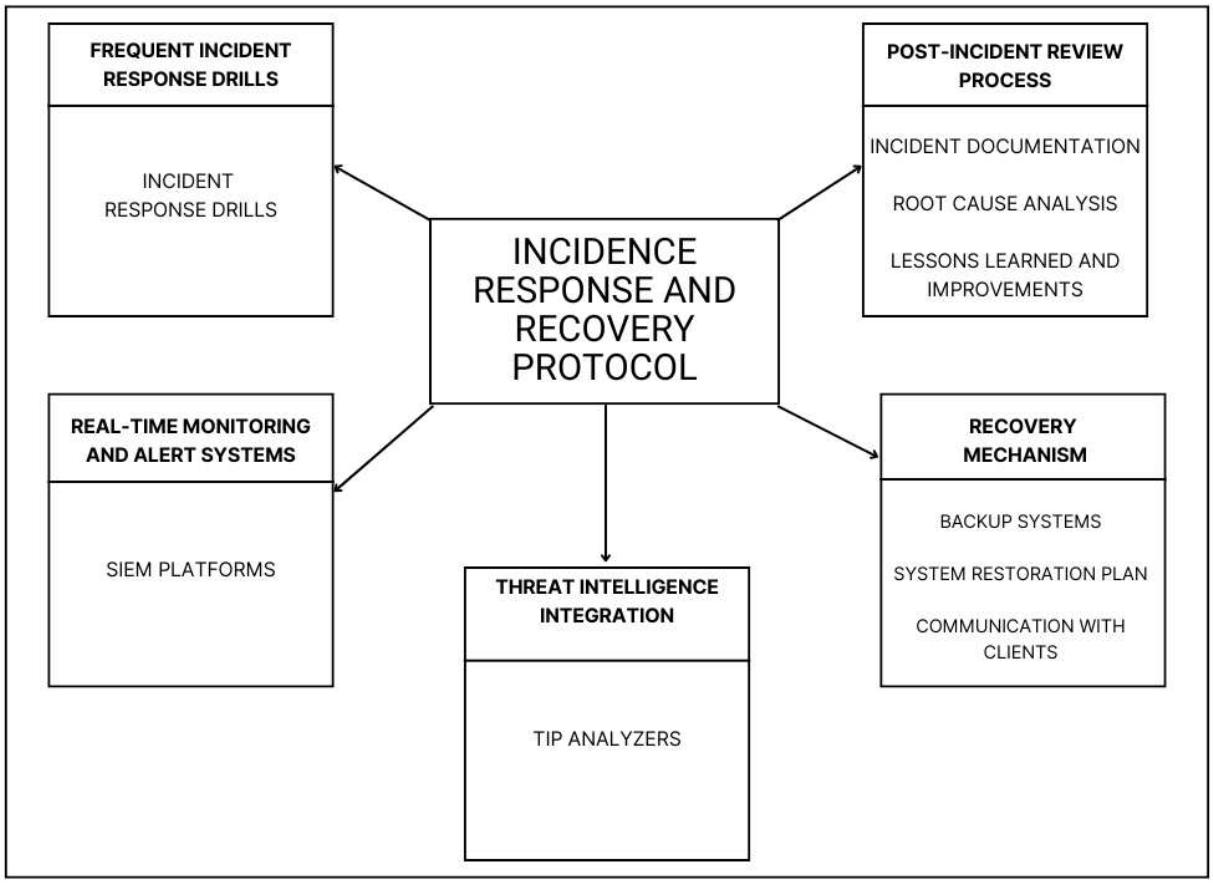

Figure 15: Illustrates the incident response and recovery protocol for Moitele

5.4.3.2 Explanation for framework Layer

- Frequent Incident Response Drills

  One of the main preventative steps is running frequent incident response exercises. These drills simulate potential security incidents such as phishing attacks, bruteforce attacks or something else. Industry research suggests that companies conducting frequent incident

response drills can reduce incident resolution time by up to 40%, minimizing the risk of prolonged operational disruption [34]. By doing a proper incident response drill, it can benefit in such a way that it increases the employee readiness and reduces panic during actual incidents, identifies weaknesses in current security processes and enhance collaborations within the different departments in the team.

- Post Incident Review Process

Post incident reviews are critical for improving future response efforts as after an incident is occurred, to investigate the main cause, evaluate the success of the reaction, and carry out required changes, Moitele should do a thorough evaluation including security teams, management, and important decision makers. Incorporating post incident reviews as a standard practice aligns with ISO/IEC 27035 guidelines, which emphasize the value of documentation and learning from incidents to enhance resilience [35]. Some of the recommendations that can be done a post incident review happened are,

- Incident Documentation: Record all relevant details such as attack vectors, compromised assets, response actions, and identified vulnerabilities
- Root Cause Analysis: Utilize forensic tools to investigate how the incident occurred and determine whether security controls were bypassed.
- Lessons Learned and Improvements: Develop actionable steps to improve security posture, such as updating firewall rules, strengthening access controls, or modifying training strategies.

- Recovery Mechanisms

Although incident containment is crucial, restoration of company activities depends equally on recovery and to have a recovery plan Moitele should focus on.

- System Restoration Plan: Establish a clear procedure for restoring systems to a trusted state with minimal data loss.
- Backup Systems: Ensure all critical data is routinely backed up in secured, geographically dispersed locations to facilitate quick recovery.
- Communication with Clients: Maintain transparent communication with clients during recovery to manage trust and minimize reputational impact.

- Threat Intelligence Integration

  To improve Moitele's resilience against evolving threats, incorporating Threat Intelligence Platforms (TIPs) is recommended, TIPs examine threat data from several sources to provide practical insights for detection and prevention strategies. By integrating threat intelligence, Moitele can proactively identify emerging risks and vulnerabilities before they influence the enterprise.

- Real Time Monitoring and Alert Systems

  Moitele should implement advanced Security Information and Event Management (SIEM) systems to guarantee the quick identification of questionable activity. These technologies instantly notify security teams of possible risks by combining security data from several endpoints. SIEM platforms can also generate automated response actions, accelerating containment and mitigation efforts.

5.4.4 Employee Training and Awareness

Employee awareness and training play a role in strengthening an organization's security posture. For Moitele, enhancing employee understanding of security risks, best practices, and incident response strategies is crucial to minimizing human errors, which are often a major factor in security breaches, Given that Moitele already maintains strong encryption standards and multifactor authentication (MFA) measures, focusing on human centric security strategies which is very good, but also will be talking about the other vulnerabilities i.e. lack of security awareness among employees.

5.4.4.1 Visual Representation for Employee Training and Awareness

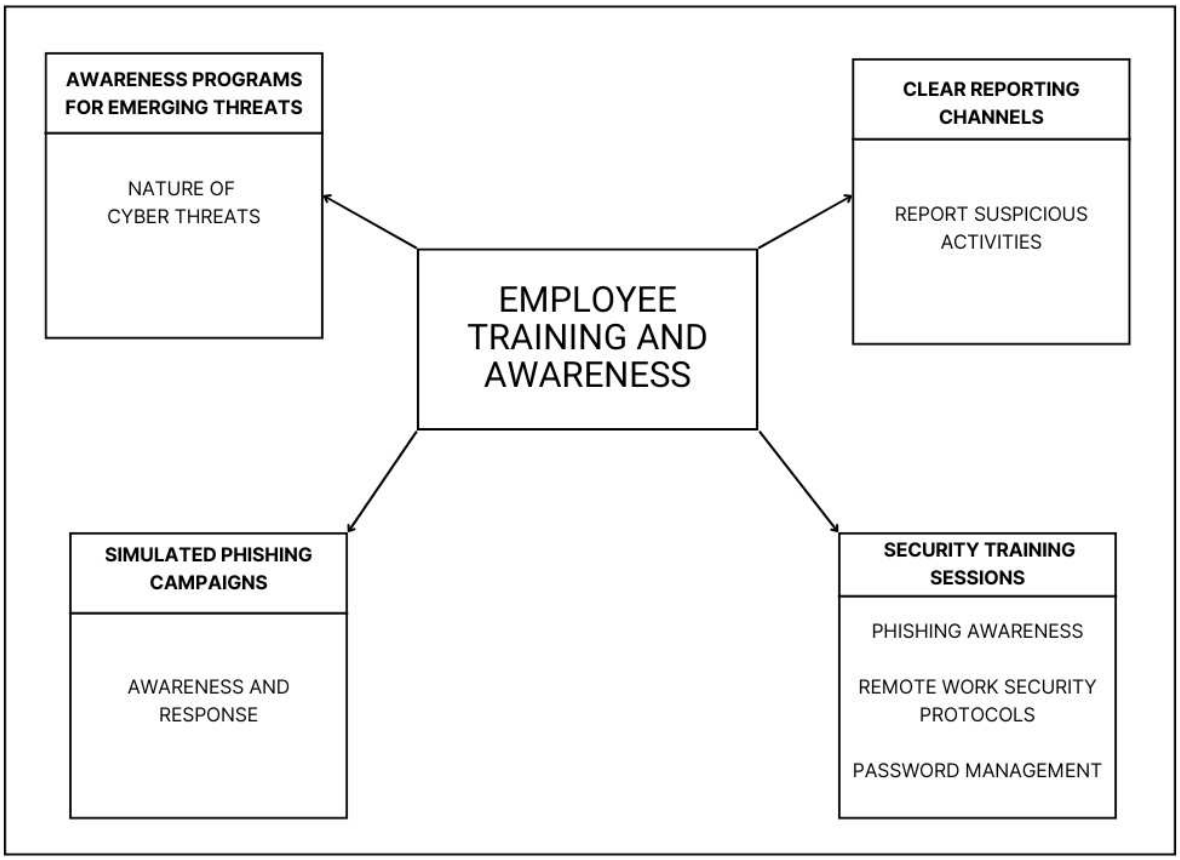

Figure 16: The figure depicts the core elements of awareness and training strategy.

5.4.4.2 Explanation for the framework layer

- Awareness Programs for Emerging Threats

  Since the nature of threats are evolving, Moitele should be conducting awareness programs to educate employees about emerging threats such as AI/ML-driven attacks, deepfake phishing scams, ransomware tactics, zero-Day Vulnerabilities are some of the evolving threats.

- Clear Reporting Channels

  Employees can quickly report suspicious activity when clear reporting routes are established. Workers should be aware of where to report questionable emails, phishing attempts, and possible insider threats. Some of the recommendations for effective reporting can be introducing a dedicated email alias (security@moitele.com) for reporting concerns, provide a secure platform where employees can submit anonymous security concerns. Encouraging employees to report potential threats significantly reduces response time and minimizes the impact of security incidents [36].

- Security Training Sessions

  Moitele should conduct comprehensive cybersecurity training programs for employees at all levels, and training must be focused on essential security practises, and this include:

  - Phishing Awareness: Employees should be trained to recognize suspicious emails, links, and attachments to prevent social engineering attacks.
  - Remote Work Security Protocols: Ensuring employees working remotely adopt secure practices like VPN usage and endpoint protection.
  - Password Management: Educate the employees the use of strong, unique passwords and secure password management tools.

- Simulated Phishing Campaigns

  Simulated phishing campaigns are highly effective in evaluating employee awareness and response to real world social engineering attacks. By sending simulated phishing emails to employees, Moitele can Identify vulnerable employees, provide coaching to improve awareness, track improvements in phishing detection rates over time. Research indicates that frequent simulated phishing campaigns reduce successful phishing attempts by 67% within six months [37].

5.5 Implementing the Proposed Security Framework in Moitele's Current Infrastructure

The proposed security framework is designed to complement Moitele's existing security infrastructure by addressing the identified gaps and enhancing the organization's overall security posture, since Moitele has a strong Multi-Factor Authentication (MFA) measures, strong encryption practices, and confidential security controls, additional layers such as Zero Trust Architecture (ZTA), AI/ML integration, improved incident response protocols, and enhanced employee awareness training are crucial as well. The recommended strategies can be effectively integrated by the following ways.

5.5.1 Zero Trust Architecture (ZTA) Implementation in Moitele

Moitele's knowledge and implementation of Zero Trust Architecture (ZTA) is currently minimal, the adoption process must follow a phased approach to ensure seamless integration.

- Phase 1: Conduct a comprehensive inventory of Moitele's cloud infrastructure, endpoints, devices, and software systems. This step is very crucial for mapping the organization's digital environment and defining security perimeters.
- Phase 2: Implement Identity and Access Management (IAM) with role-based access control (RBAC) to ensure only authorized personnel can access sensitive data. Secondly, introduce User and Entity Behaviour Analytics (UEBA) to monitor user behaviour patterns and flag unusual activity.
- Phase 3: Establish PEP systems at key network gateways to verify all traffic based on identity, device, and contextual data before granting access, enforce the "Never Trust, Always Verify" principle.
- Phase 4: Utilize real-time monitoring tools to identify suspicious activity and respond immediately.
- Phase 5: Before expanding ZTA across the entire organisation, implement it in key business units as a start.

5.5.2 AI/ML Integration in Moitele

Since Moitele hasn't not yet adopted AI/ML solutions, and this is considered to the most important phase as of now. To do this, it can be implemented in a phased approach.

- Phase 1: As the initial stage, Integrate User and Entity behaviour Analytics (UEBA) solutions to monitor user behaviour, detect deviations, and flag potential threats or compromised accounts, Moitele can use AI based monitoring solutions such as crowd strike, Darktrace based on the budget.
- Phase 2: Deploy tools that analyse network traffic patterns and alert teams about potential brute force attacks or DDoS threats. Certain detection tools are Splunk, Exabeam etc.
- Phase 3: Implements Natural Language Processing (NLP) systems to analyse suspicious emails and malicious URLs to prevent phishing attacks, secondly introduce automated incident response systems.

5.5.3 Incident Response and Recovery Protocols

While Moitele's existing security controls include incident prevention, incident response mechanisms need strengthening to minimize downtime and data loss in the event of a breach. Implementation should include

- Conduct quarterly simulation exercises that mimic attack scenarios to ensure employees are equipped to respond effectively, effectively use frameworks like the NIST Cybersecurity Framework **or** MITRE ATT&CK to design comprehensive drills.
- Introduce review mechanism that documents the timeline of incidents, identifies root causes, and evaluates incident handling. A recommended tool would be SIFT Workstation.
- Develop a playbook that outlines incident response workflows, escalation procedures, and contact points for Moitele's security teams.

5.5.4 Employee Awareness and Training

To reduce human error and improve security readiness, Moitele should expand its employee security awarenesses and these can be done by

- Asking employees to subscribe or follow certain content that follows latest security challenges and recent attacks, try to implement some awareness programs on a quarterly basis.
- Designate a secure and accessible reporting mechanism where employees can promptly report suspicious activities.
- Develop specialized training modules for technical staff, developers, and non-technical employees based on their exposure to security risks.

5.6 Implementation Blueprint

The success of any security framework depends not only on design but also on how effectively it is implemented within the existing infrastructure. This outlines a phased and layered deployment strategy for integrating the proposed security framework in midsized cloud communication companies.

	Phase	Focus Area	What to Implement	Recommended Toos
	Phase 1	Identity & Access Management (IAM)	Centralized IAM, MFA, SSO, RBAC	Okta, Azure AD, Google Workspace
	Phase 2	Zero Trust Architecture (ZTA)	Micro-segmentation, contextual access, device trust	Zscaler, Cisco Duo, Beyond Corp
	Phase 3	AI/ML-Powered Threat Detection	Behavioural analytics, anomaly detection, automated alerting	CrowdStrike, Defender, Darktrace
	Phase 4	Data Encryption & Blockchain	End-to-end encryption, blockchain for logging	TLS 1.3, AES-256, Hyperledger
	Phase 5	SIEM and Monitoring	Centralized log collection, automated detection and alerting	Splunk, ELK Stack, Azure Sentinel

5.6.1 Phases Explanation

Implementing a strong security framework in cloud communication companies demands a carefully phased approach. This ensures that the strategy aligns with organizational goals, is technically and operationally practical, and is supported by adequate preparation across the company. The following blueprint outlines five structured stages to guide this process:

Phase 1: Assessment and Planning

This initial phase involves a comprehensive evaluation of the current security posture, identifying vulnerabilities, compliance gaps, and misalignments with best practices and these includes:

- Risk Assessment: These includes identifying and categorizing threats based on their likelihood and impact [42].
- Security Audits: Reviewing the existing tools, policies, and controls in place in accordance with frameworks like ISO/IEC 27001 [44].
- Strategic Planning: Defining security objectives aligned with business goals, resource planning, and stakeholder involvement.
- Gap Analysis: Comparing the current state to industry standards such as NIST SP 800-37 and CIS Controls [42][8].

Phase 2: Foundation and Architecture Design

This second phase focuses on designing the technical architecture and foundational controls based on the assessment results:

- Security Architecture Design: Develop a high-level architecture covering identity, access, data flow, and perimeter security [45].
- Zero Trust Blueprinting: These includes designing micro-segmentation, policy enforcement points, and continuous verification mechanisms, aligned with the NIST Zero Trust Architecture model [43].
- Tool Selection and Acquisations: These includes identifying necessary technologies such as IAM systems, endpoint protection, and threat monitoring tools [46].

- Policy and Governance Framework: Establishing security policies, compliance controls, and data governance models grounded in ISO/IEC 27001 standards [44].

Phase 3: A Prototype Deployment

Before launching out the framework organization wide, a prototype deployment is essential to validate assumptions and refine configurations:

- Key Controls: Implementing key controls and technologies in a test environment [45].
- Training and Awareness: Conducting training sessions for relevant teams on new systems and protocols.
- Performance Benchmarking: Evaluating tool effectiveness, response times, and alert accuracy [47].
- Feedback and Updating: Collecting user and system feedback to fine updating the configurations and ensure operational readiness.

Phase 4: Full Implementation

Once the prototype is validated, the full implementation takes place across all systems, teams, and data layers:

- System Integration: Deploying solutions across cloud infrastructure, endpoints, applications, and network components [45].
- Incident Response Enablement: Aligning incident response protocols with frameworks like those proposed by SANS and NIST [48].
- Policy Enforcement: Enabling role-based access control (RBAC), least privilege policies, and multi-factor authentication (MFA) in alignment with Zero Trust principles [43].
- Continuous Monitoring: Implementing SIEM/SOAR platforms for real-time threat detection and response [45].

Phase 5: Continuous Improvement and Compliance

This final phase is to establish an ongoing process of evaluation, adaptation, and improvement and this include:

- Threat Intelligence Integration: Utilising global threat feeds and integrating with existing SIEM tools for enhanced detection [49].
- Compliance Audits: Ensuring continuous alignment with GDPR, HIPAA, and ISO 27001 standards [44].
- Periodic Penetration Testing: Validating defence capabilities through ethical hacking simulations.
- Feedback Loop: Regularly reviewing incidents, user feedback, and audit findings to update the framework and reinforce security posture.

Implementing a security framework in a steady and well-structured manner helps to maintain operational stability while allowing the organisation to respond to emerging cyber threats and regulatory requirements. Each stage, from initial evaluation to design, full deployment, and continuous tuning, builds on the previous one, resulting in a robust and layered defence system.

6 Conclusion and Recommendations

6.1 Conclusion

The research carried out in this thesis aimed to analyze the existing security posture of Moitele, a cloud communication company, and propose a comprehensive security framework tailored to address identified gaps and vulnerabilities within the organizations and it was conducted through a combination of quantitative and qualitative data, key security concerns, strengths, and improvement areas were identified.

6.1.1 Findings

6.1.1.1 Moitele's Strength

The company has implemented multi-factor authentication (MFA) measures, ensuring strong access control. Additionally, data encryption protocols are also enforced, ensuring data confidentiality during transmission. These implementations align with industry best practices, strengthening Moitele's foundational security posture.

6.1.1.2 Identified Gaps

These research findings revealed that Moitele has minimal awareness and no current implementation of Zero Trust Architecture (ZTA), which shows a risk in access control and lateral movement threats. The absence of AI/ML integration was also highlighted, limiting the company's ability to proactively detect and mitigate advanced threats. Furthermore, while Moitele has established some sensitive security measures, there were clear gaps in employee awareness programs and structured incident response plans.

6.1.1.3 Impact of the Findings

The findings highlight the necessity for significant upgrades in Moitele's security infrastructure. Without adopting proactive security measures such as ZTA and AI-driven solutions, Moitele remains vulnerable to evolving cyber threats. Enhancing employee training, refining incident response strategies, and introducing modern security frameworks are critical steps for improving overall security resilience.

6.2 Recommendations

This section presents targeted recommendations for mid-sized cloud communication service providers, grounded in the data collected from surveys and expert interview. The proposals are intended to address recognised gaps in awareness, technological adoption, and operational readiness, while also facilitating scalable implementation.

- Implement Zero Trust Architecture (ZTA)

  The study highlighted a low level of awareness and non-adoption of Zero Trust principles irrespective of the organization strengths. Organizations should prioritize transitioning from traditional security measures to a Zero Trust model, where verification is required for every user and device accessing resources, regardless of network. This involves micro segmentation, least privilege access, and continuous context aware validation. Tools such as identity aware proxies and policy enforcement points can be integrated gradually to minimize disruption.

- Strengthen Employee Awareness and Security Training

  The quantitative analysis revealed limited concern about insider threats and inconsistent encryption practices, suggesting a gap in employee awareness. Regular cybersecurity awareness programs, simulated phishing attacks, and interactive workshops should be deployed to build a security conscious culture. Focus areas should include:

  - Recognizing social engineering threats
  - Following secure communication protocols
  - Understanding organizational security policies

- Adopt AI/ML-Driven Threat Detection Tools

  Organizations still relying on traditional rule-based security monitoring are at risk of missing sophisticated, real-time threats. The adoption of AI and Machine Learning solutions can help detect anomalous behaviour and automate response strategies. These tools can also enhance visibility into low and slow attacks, insider threats, and endpoint anomalies.

- Establish Structured Incident Response Frameworks

  A well-documented and frequently tested Incident Response Plan (IRP) is critical. The plan should define responsibilities, escalation paths, containment procedures, and recovery strategies. Periodic tabletop exercises and red team simulations should be conducted to test the plan's effectiveness. Aligning with NIST SP 800-61 or ISO/IEC 27035 is recommended to ensure coverage of all incident response phases.

- Deploy a Centralized Monitoring and Alerting System (SIEM)

  Visibility across cloud and on premises environments is essential. Implementing a Security Information and Event Management (SIEM) system can centralize log collection, perform threat correlation, and trigger alerts for suspicious activities. SIEM platforms also support compliance reporting and incident forensics, making them an integral part of proactive defence strategies.

- Enforce End-to-End Data Encryption and Explore Blockchain Integration

  To secure data confidentiality and integrity, organizations must adopt robust encryption techniques such as TLS 1.3 for data in transit and AES-256 for data at rest. Additionally, blockchain can be used to ensure tamper resistant logging and data validation, particularly for authentication records and audit trails. Although its implementation is still emerging, it represents a valuable layer for long-term security strategy.

These recommendations help in assisting cloud communication companies like the one studied in this thesis in maturing their security framework, aligning with evolving threat landscapes and compliance requirements. A phased and adaptable approach is suggested, ensuring minimal operational disruption while maximizing long term resilience

6.3 Future Research Directions

While this thesis focused on security solutions specifically tailored for midsized cloud communication company, future research can expand upon several key areas

- Longitudinal Study on Framework Effectiveness

Future research can involve tracking the real-world implementation of the proposed security framework over time. Longitudinal studies can measure how adopting Zero Trust, AI/ML tools,

and centralized monitoring impacts threat detection rates, incident response times, and user behaviour.

- AI/ML Security Tool Evaluation

  There is a growing need to critically assess the effectiveness, accuracy, and explainability of AI/ML based threat detection systems. Researchers could benchmark different platforms, evaluate their false positive rates, and explore model transparency, especially in cloud native environments.

- Comparative Studies Across Providers

  This thesis focused on a single organization. A broader study comparing multiple cloud communication service providers across varying sizes, sectors, and regions would provide a more comprehensive view of industry wide security practices, adoption barriers, and operational maturity.

- Regulatory and Legal Compliance Integration

  As regulations like GDPR, CCPA, and NIS2 Directive evolve, future studies could investigate how cloud providers integrate legal compliance with technical security controls. A particular focus on cross-border data flow**,** auditability**,** and privacy enhancing technologies (PETs) would be highly relevant.

This future research roadmap serves as a foundation for building more robust, adaptive, and research driven security strategies for cloud communication firms navigating an increasingly complex threat landscape.

References

[1] Cloud Security Alliance, Cloud Controls Matrix (CCM) v4.0, 2021. [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4

[2] Ponemon Institute, Cost of a Data Breach Report 2021, IBM Security, 2021. [Online]. Available: https://www.ibm.com/security/data-breach

[3] J. Kubacz-Szumska and O. Szumski, "Cloud Communications During the Pandemic from the Perspective of Collaboration Platforms," Problemy Zarządzania, vol. 19, no. 3 (93), pp. 105–123, 2021, doi: 10.7172/1644-9584.93.5. [Online]. Available: https://doi.org/10.7172/1644-9584.93.5

[4] E. Shunmugam, "Privacy Ensuring SRTP for Cloud Conferencing," M.S. thesis, School of Computer Science and Communication, KTH Royal Institute of Technology, Stockholm, Sweden, 2016. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-193438

[5] E. Rescorla and B. Adkins, "WebRTC Security Architecture," RFC 8827, Internet Engineering Task Force, May 2021. doi: 10.17487/RFC8827. [Online]. Available: https://datatracker.ietf.org/doc/rfc8827/

[6] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization, 2022. [Online]. Available: https://www.iso.org/standard/82875.html

[7] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[8] Cloud Security Alliance, Cloud Controls Matrix (CCM) v4.0, 2024. [Online]. Available: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4

[9] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR)," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] State of California Department of Justice, California Consumer Privacy Act (CCPA), 2018. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[11] National Institute of Standards and Technology, "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020. doi: 10.6028/NIST.SP.800-207. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[12] SentinelOne, "17 Security Risks of Cloud Computing in 2024," SentinelOne Cybersecurity 101, 2024. [Online]. Available: https://www.sentinelone.com/cybersecurity-101/cloud-security-risks-2024/

[13] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025. [Online]. Available: https://doi.org/10.1016/j.ins.2015.01.025

[14] M. Alshahrani and R. Simpson, "Evaluating the Effectiveness of Multi-Factor Authentication in Cloud Security," International Journal of Information Security, vol. 25, 2023. [Online]. Available: https://doi.org/10.1007/s10207-023-00705-1

[15] T. Keary, "Report shows 92% of orgs experienced an API security incident last year," VentureBeat, Oct. 17, 2023. [Online]. Available: https://venturebeat.com/security/report-api-security-incidents-2023/

[16] R. K. Khatoun and S. Zeadally, "Cybersecurity and privacy solutions in smart cities," IEEE Communications Magazine, vol. 55, no. 3, pp. 51–59, Mar. 2017, doi: 10.1109/MCOM.2017.1600297CM. [Online]. Available: https://doi.org/10.1109/MCOM.2017.1600297CM

[17] Cloudflare, "How to prevent DDoS attacks," Cloudflare Learning Center. [Online]. Available: https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/

[18] Deloitte, "The future of cybersecurity and AI," Deloitte Insights, 2022. [Online]. Available: https://www2.deloitte.com/us/en/insights/industry/technology/future-of-cybersecurity-and-ai.html

[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A Survey of Deep Learning Methods for Cyber Security," Information, vol. 10, no. 4, p. 122, Apr. 2019, doi: 10.3390/info10040122. [Online]. Available: https://doi.org/10.3390/info10040122

[20] Z. Li, A. L. G. Rios, and L. Trajković, "Machine Learning for Detecting Anomalies and Intrusions in Communication Networks," IEEE Journal on Selected Areas in Communications, vol. 39, no. 7, pp. 2254–2264, July 2021, doi: 10.1109/JSAC.2021.3078497. [Online]. Available: https://doi.org/10.1109/JSAC.2021.3078497

[21] Vinsys, "Top 20 Emerging Cybersecurity Trends to Watch Out in 2024," Vinsys Blog, Oct. 17, 2023. [Online]. Available: https://www.vinsys.com/blog/emerging-cybersecurity-trends-2024/

[22] S. Bhattacharya, M. Najana, and A. Khanna, "Decentralized Identity Verification via Smart Contract Validation: Enhancing PKI Systems for Future Digital Trust," International Journal of Global Innovations and Solutions (IJGIS), vol. 3, no. 1, pp. 15–23, 2024. [Online]. Available: https://ijgis.com/article/view/2024/identity-verification-smart-contracts

[23] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, Aug. 2020, doi: 10.6028/NIST.SP.800-207. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[24] M. Blessing, W. Kolawole, and J. Owen, "The Role of Zero Trust Architecture in Enhancing Cloud Security for Enterprises," ResearchGate, 2024. [Online]. Available: https://www.researchgate.net/publication/380710591_Zero_Trust_Architecture_in_Cloud_Security

[25] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed. Thousand Oaks, CA: SAGE Publications, 2018. [Online]. Available: https://us.sagepub.com/en-us/nam/research-design/book255675

[26] F. J. Fowler Jr., Survey Research Methods, 5th ed. Thousand Oaks, CA: SAGE Publications, 2018. [Online]. Available: https://us.sagepub.com/en-us/nam/survey-research-methods/book245525

[27] J. Pallant, SPSS Survival Manual: A Step-by-Step Guide to Data Analysis Using IBM SPSS, 7th ed. New York, NY: McGraw-Hill, 2020. [Online]. Available: https://www.mheducation.com/highered/product/spss-survival-manual-pallant/M9780335249497.html

[28] A. Field, Discovering Statistics Using SPSS, 5th ed. Thousand Oaks, CA: SAGE Publications, 2018. [Online]. Available: https://us.sagepub.com/en-us/nam/discovering-statistics-using-ibm-spss-statistics/book260423

[29] A. Gibbs, “NVivo in qualitative research,” in Research Methods in Social Sciences, 3rd ed., A. Tashakkori and C. Teddlie, Eds. Thousand Oaks, CA: SAGE Publications, 2015, ch. 12, pp. 322–335.

[30] Verizon, Data Breach Investigations Report 2023, Verizon Enterprise, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/Verizon+1broadband.masstech.org+1
[31] National Institute of Standards and Technology, "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020. doi: 10.6028/NIST.SP.800-207.
[32] D. Johnson, "The Role of Least Privilege in Preventing Insider Threats," International Journal of Cybersecurity Strategies, vol. 12, no. 2, pp. 20–29, 2023. [Online]. Available: https://ijcss.com/article/view/least-privilege-insider-threats
[33] J. Garcia and C. Williams, "Micro-segmentation for Enhanced Security," Journal of Cyber Defence, vol. 45, no. 3, pp. 55–63, 2022. [Online]. Available: https://jcdjournal.com/article/microsegmentation-security
[34] J. Shackleford, "The Impact of Incident Response Drills on Cybersecurity Resilience," Journal of Information Security Management, vol. 18, no. 3, pp. 45–58, 2021. [Online]. Available: https://jism.org/articles/incident-response-drills-resilience
[35] International Organization for Standardization (ISO), "ISO/IEC 27035: Information Security Incident Management," 2021. [Online]. Available: https://www.iso.org/standard/74033.html
[36] J. O'Hara, "Incident Reporting Practices and Security Resilience," Security Awareness Review, vol. 9, no. 4, pp. 42–58, 2020. [Online]. Available: https://securityawarenessreview.org/articles/incident-reporting-resilience
[37] C. Bradley, "Evaluating the Impact of Simulated Phishing Exercises in Corporate Environments," International Journal of Cybersecurity, vol. 12, no. 3, pp. 85–99, 2021, doi: 10.1007/s10207-021-00540-9.
[38] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," Journal of Cloud Computing, vol. 9, no. 1, pp. 1–18, 2020, doi: 10.1186/s13677-020-00177-x.
[39] Amazon Web Services, "Shared Responsibility Model," AWS Whitepaper, 2023. [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/
[40] Gartner, "Is the Cloud Secure?" Gartner Research, May 2022. [Online]. Available: https://www.gartner.com/en/documents/4001234
[41] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, vol. 305, pp. 357–383, June 2015, doi: 10.1016/j.ins.2015.01.025.
[42] NIST, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," NIST Special Publication 800-37 Revision 2, Dec. 2018. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-37r2
[43] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207
[44] SO/IEC, "ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements," International Organization for Standardization, 2022.
[45] Cloud Security Alliance (CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 2017. [Online]. Available: https://cloudsecurityalliance.org/research/guidance/
[46] Gartner, "IAM Leaders' Guide to Identity Governance and Administration," Gartner Research, 2021. [Online]. Available: https://www.gartner.com/
[47] S. Chuvakin and A. Zeltser, "How to Deploy SIEM for Security Monitoring," Gartner Research, 2019.

[48] SANS Institute, “Incident Handler's Handbook,” SANS Institute Reading Room, 2021. [Online]. Available: https://www.sans.org/white-papers/incident/

[49] Center for Internet Security (CIS), “CIS Controls v8,” CIS, 2021. [Online]. Available: https://www.cisecurity.org/controls

[50] KongHQ, “APIs Are Mission Critical in Modern Enterprises,” *KongHQ Blog*, Feb. 2024. [Online]. Available: https://konghq.com/blog/enterprise/apis-are-mission-critical

f Akamai, “DDoS Attacks Rising Faster in EMEA than Anywhere Else, According to New Akamai Report,” Akamai Newsroom, Apr. 2024. [Online]. Available: https://www.akamai.com/newsroom/press-release/ddos-attacks-rising-faster-in-emea-than-anywhere-else-according-to-new-akamai-report

[52] Cloud Security Alliance, “An Analysis of the 2020 Zoom Breach,” Cloud Security Alliance Blog, Mar. 2022. [Online]. Available: https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach

[53] Brier & Thorn, “Incident Review: Twilio Smishing Attack,” *Brier & Thorn Blog*, Aug. 2022. [Online]. Available: https://www.brierandthorn.com/post/incident-review-twilio-smishing-attack

[54] McKinsey & Company, “The Role of AI in Enhancing Cybersecurity Strategies,” 2023. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer

[55] Precedence Research, “Artificial Intelligence Market Size,” *Precedence Research*, 2024. [Online]. Available: https://www.precedenceresearch.com/artificial-intelligence-market

[56] Market.us, “Global Encryption Software Market Size, by Component, 2023–2033 (USD Billion),” *Market.us*, 2024. [Online]. Available: https://market.us/report/encryption-software-market/

[57] Core Security, “2019 Identity and Access Management (IAM) Report,” *Core Security*, 2019. [Online]. Available: https://www.coresecurity.com/resources/guides/2019-iam-report

[58] SlideTeam, *Blockchain Integrated Cloud Computing - Decoding Blockchain Integration*, SlideTeam.net. [Online]. Available: https://www.slideteam.net/blockchain-integrated-cloud-computing-decoding-blockchain-integration-ppt-presentation-bct-ss-v.html

[59] A. Author, “Title of the Article,” *European Journal of Engineering*, vol. X, no. X, pp. XX–XX, 2023. [Online]. Available: https://www.ejeng.org/index.php/ejeng/article/view/3074

[60] Market.us, “Global Identity and Access Management Market Report,” Market.us, 2024. [Online]. Available: https://market.us/report/identity-and-access-management-market/