National College of Ireland

Securing the cloud: Integrating Zero Trust, Threat Detection, and Encryption

MSc Research Project
Cloud Computing

Bhanu Prakash Palukuri
Student ID: 23413999

School of Computing
National College of Ireland

Supervisor: **Shaguna Gupta**

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Bhanu Prakash Palukuri
Student ID:	23413999
Programme:	Cloud Computing **Year:** 2026
Module:	**MSc Research Project**
Supervisor:	**Shaguna Gupta**
Submission Due Date:	28/1/2026
Project Title:	Integrating Zero Trust, Threat Detection, and Encryption

Word Count: **Page Count:27**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing the Cloud: Integrating Zero Trust, Threat Detection, and Encryption

Bhanu Prakash Palukuri
23413999

January 28, 2026

Abstract

The expansion of cloud computing has widened the different operations and, at the same time, appears to increase the incidence of security risks since the traditional framework is inadequate in identifying the activities of child misuse of credentials, insider attack, and information exfiltration. In order to investigate the embedded integration of Zero Trust Architecture (ZTA), Threat detection, and encrypted data processing to promote the security of cloud-based enterprise settings, this research paper introduces an in-depth analysis based on perceived inputs. The supplementary laboratory simulations are provided under discrete cloud setups as an imitation of credential abuse, lateral movement, and controlled strain situations.

The performance overhead of integrated security strategies, along with detection accuracy and containment capabilities, is evaluated at the empirical level. The work is conducted in strict alignment with the protocols set in the field of research and took the ethical responsibility on itself, such that confidential information is anonymised with full control to ensure no confidential information was disclosed. The mechanisms of institutional governance ensure the audit controls of the investigative process. The result is predicted to be a unified security level achieved by the integration of all the advantages of ZTA, system surveillance, and encryption. This theoretical framework is designed to close the gap between theoretical studies and their practical application by outlining a systematic approach toward the development of the integration of Zero-Trust-Architecture, proactive monitoring, and encryption technologies.

***Keywords*— Zero Trust Architecture, Threat Detection, Encrypted Data Processing, Cloud Security, Cyber Threat Simulation**

1. Introduction

1.1 Background of the Study

Enterprise cloud computing is being adopted relatively low in general, but almost 94 per cent of organisations have adopted cloud services with the aim of improving efficiency and scalability of their operation (Faruque et al. 2024). This adoption has, however, been accompanied by a very strong rise in cyberattacks with a view to stealing crucial information and systems in enterprises. The conventional perimeter-based security architectures are becoming increasingly incapable of traditional high-risk threats such as identity theft, cross-border attacks, and exfiltration of data. Recent advancements and improvements include upcoming paradigms, including Zero-Trust Architecture, Threat detection, and encrypted data processing as individual and powerful defensive mechanisms (Tiwari et al. 2022). The traditional perimeter-based security measures do not help to deal with the emerging threats, such as credential abuse, brute force attacks, insider attacks, and massive data leaks, since they cannot scale to track and respond to threats that start in the very cloud. Zero-trust designs, Threat detection, and encrypted data processing have become the main mitigation strategies that are expected to be adopted in the future (Laghari et al. 2025).

1.2 Research Aim and Objective

Aim

The research purpose is to identify the efficiency of the integration of the Zero Trust Architecture, AI-based monitoring, and encrypted data processing to enhance the security level of the cloud-based enterprises.

Objectives

- To design and implement a simulation-based cloud security architecture integrating Zero Trust principles, encrypted data processing, and network isolation mechanisms
- To experimentally evaluate the operational effectiveness of the proposed architecture within a controlled cloud simulation environment
- To measure and analyse the framework's effectiveness in detecting and mitigating key cloud security threats, including credential abuse, lateral movement, brute-force attacks, and denial-of-service attacks
- To assess the scalability, resilience, and compliance readiness of the proposed framework using systematic performance monitoring and stress-testing within the simulation environment

1.3 Research Questions

How effective is the combined implementation of Zero Trust Architecture, AI-driven threat detection, and encrypted data processing in mitigating advanced security threats to sensitive data in enterprise cloud environments?

1.4 Scope of the Research

The scope of the research is the analytical discussion of the possibility of putting into practice the Zero Trust Architecture, monitoring, and encoded data processing in enterprise clouds. Simulated scenario analysis is performed in controlled laboratory experiments, which involve artificialized profiles of credit-abusers, or systematic tests to stress the performance of systems, thus intentionally avoiding interaction with working systems (Harrison et al. 2024). The research does not use primary data of organisations, which means that the available literature, case studies, and other secondary resources also offer the viability, scalability, and compliance risk of an integrated cloud security framework.

1.5 Summary

Cloud computing possesses scalability and efficiency; however, it faces the challenge of constant security threats. The current models are too deficient to capture diverse risks such as misuse of credentials and breaches of data. The research helps to understand the relevance of the topicality of the principles of the so-called Zero Trust and the use of artificial intelligence-based monitoring and encryption during the work on the design and implementation of resilient, scaled, and compliance-oriented enterprise cloud security systems using both qualitative and quantitative research strategies.

1.6 Project Structure

There are seven sections in this project. The introduction section provides the background of the research, problem statement, and objectives. The literature review section summarises the available research and identifies gaps in research. The methodology section has the description of the research design, tools, and experimental approach. The system security framework and architecture are outlined in the Design Specification section. The implementation section has the description of the AWS-based setup and security configurations.

The evaluation section contains experiments, measures, findings, and comparisons. The Conclusion and Future Work section is a conclusive note and work improvement.

2. Literature Review

Cloud computing has increased the pace of digital transformation. The principle of Zero Trust helps to improve access control, artificial intelligence helps to detect threats more adaptively, and encryption helps to protect the integrity of data. Despite these innovations, the majority of the research is based on individual technologies and does not consider how they can be deployed in multi-faceted clouds. This review evaluates the approaches published to date critically, reviews their advantages and disadvantages, and analyses the gaps that lead to an integrated security framework to combine Zero Trust, AI, and encryption.

2.1 Zero-Trust Architectures in Cloud Environment

2.2.1 Zero-Trust Architectures in Multi-Cloud

The Zero Trust Architecture (ZTA) has been a growing subject of cloud security studies, even in terms of how to support the trust assumptions of distributed and multi-cloud environments. Anasuri, (2022), considers the usability of ZTA on heterogeneous cloud platforms and shows that the elimination of implicit trust can significantly lower attack surfaces in contrast to perimeter-based frameworks of the past. Although the study reports about better security postures in a multi-cloud deployment, it is in much of its conceptual concepts not empirically confirm performance overheads or consistency of enforcement among the various cloud service providers.

In comparison to the previous cloud security architectures, the work by Anasuri focuses on the issues of interoperability caused by provider-specific identity and access control in the case of multi-cloud environments, which makes it difficult to apply homogeneous policies. Since the research suggests the implementation of artificial intelligence to increase the adaptive ability of threat detection, it fails to present a specific implementation framework or comparative analysis with AI-enabled ZTA models. Although the study confirms that ZTA is a better conceptual choice to confine to a multi-cloud security system, it reveals an underlying gap in its practical application and practical effectiveness in terms of scale.

2.2.2 Combining Cloud Security with Zero Trust

The Zero Trust security model functions on the principle of constant validation, whereas traditional perimeter-based security models assume internal network trust and threats are constant. According to Damaraju, (2022), a security system based on the implementation of the principles of the Zero Trust policy in a cloud setting, in the form of strict authentication, limited privileges, permanent monitoring, encryption, and network isolation, offers more effective protection against insider threats and misuse of credentials than perimeter-oriented protection. Although the paper uses the idea of the Zero Trust as being a more advanced paradigm of architecture, the focus is more on designing principles rather than directly pointing to the real operational and performance overhead, or scalability in the multi-cloud case.

Despite the best practices mentioned by Damaraju in the context of implementing the Zero Trust controls, little emphasis is placed on the practical issues of enforcing the same policies of identity and accessibility in a heterogeneous cloud platform. The suggested integration framework provides strategic direction but does not have the quantitative data to prove its usefulness in comparison to the conventional or hybrid cloud security frameworks, especially in large-scale or dynamically evolving infrastructure.

2.2.3 Redefining Cloud Networks' Zero Trust Architecture

Zero Trust Architecture (ZTA) presupposes that no trust is implied, and any user, device, or application can be checked at any time under the location of the applications. According to Ike et al.(2021), real-time policy enforcement with user behaviour analytics, device integrity, and environmental context, as added to with identity and access management, multi-factor authentication, and security at the micro services level.

The interpretation of dynamic ZTA educates the creation of dynamic cloud security approaches. The understanding of granular, context-aware controls helps to implement accurate access control, real-time monitoring, and AI-assisted policy implementation to perform a high level of protection in the environment of multi-cloud and hybrid systems.

2.2.4 AI-Driven Zero-Trust Security Frameworks for Cloud Infrastructure

According to Parisa et al. (2023), Zero Trust security models based on AI improve traditional cloud security by performing continuous checks of users, devices, and applications, engaging AI to detect anomalies, automatically limit threats, and enable adaptive management. Security posture is further enhanced with the help of integration with such compliance frameworks as GDPR and PCI-DSS.

The ideas of AI-derived Zero Trust models inform the development of smart security architectures on retail cloud systems, with its focus on the continuous authentication, dynamic execution of policies, and the use of AI to respond to threats. The integration of these principles involves efficient, resilient, and scalable cloud security to resolve high-level cyber-attacks in hybrid and multi-cloud conditions.

2.2.5 Probability-Based Authentication and Zero Trust Architecture to Maintain Cloud Data Security and Privacy

According to Colomb et al. (2022), cloud environments require more than perimeter-based defences and result in security vulnerabilities such as information breaches and unauthorised lateral movement within the networks. Zero Trust (ZT) architecture and Policy-Based Authentication (PBA) have also been suggested to facilitate greater levels of protection of data through the creation of strict access controls and involving constant verification.

The mentioned work is very relevant to the project goal of ensuring data safety within cloud computing systems. The prioritisation of the Zero Trust architecture, encryption, and behavioural monitoring contributes to the creation of fluid security frameworks. Combining these principles guarantees a defensive proactive system to secure sensitive organisational data at the same time, remaining compliant and efficient in its operation.

2.2 AI-driven Threat Detection in Cloud Environments

2.2.1 An extensive analysis of AI-powered detection methods

Machine learning (ML), deep learning (DL), and metaheuristic algorithms of AIs have reshaped the field of cyber-attack detection because these allow real-time threat identification, anomaly detection, and adaptive intrusion prevention. According to Salem et al. (2024), DL is a proficient supercomputer in identifying complicated, nonlinear trends, identifying threats that were unfamiliar before, and advancing Advanced Persistent Threat (APT). ML automates behaviour analysis based on network traffic, and metaheuristics search the feature space and hyperparameters to achieve better results.

The knowledge gained through threat detection using AI is used to build smart Zero Trust security infrastructures in retail clouds. The integration of ML, DL, and metaheuristics will improve continuous

authentication, adaptive access control, and automated threat mitigation to ensure responsive, scalable, and robust cloud security against the new cyber threats.

2.2.2 AI-Driven Threat Detection

Detection of AI-based threats uses machine learning (ML) and deep learning (DL) to detect cyber-attacks in real-time. According to Khan et al. (2004), it has been identified that the capability of the AI to identify zero-day exploits, polymorphic malware, insider threats, user behaviour, and network traffic anomalies.

Anomaly detection and mitigation, and proactive cloud and retail responses to anomalies are available with insights based on the AI-driven detection, which is essential in creating intelligent Zero Trust security models using these insights. A combination of ML and DL increases responsiveness, operational performance, and tolerance to changing cyber-threats.

2.2.3 AI-Based Threat Identification and Response

Threat detection and response proposed by AI using machine learning and deep learning algorithms is commonly advertised as a transition towards reactive to proactive cybersecurity. Yaseen, (2023) further justifies that AI systems have more advantages compared to traditional rule-based detection by evaluating large volumes of data, detecting out-of-place behaviour, and predicting the evolution of a threat. Although this is an obvious benefit relative to signature-based systems that do not cope with zero-day attacks, the research greatly presupposes the data quality consistency and models' reliability, which cannot be guaranteed in a dynamic cloud setup.

Even though the introduction of AI-assisted observability and automated response is suggested as a facilitator of intelligent Zero Trust Architectures, little empirical data is presented to support their role in minimising response time or false positives when implemented in real cloud environments. This raises questions on the transparency of operations, model bias, and scalability of automated retaliation systems, especially on complex five-tenant or more cloud systems.

2.2.4 Using zero-trust architecture and cloud-based AI to improve US cybersecurity and counteract global threats

According to Kolawole, (2024), the combination of cloud-based artificial intelligence (AI) and Zero Trust Architecture (ZTA) represents the revolutionary measures to enhance American cybersecurity. The research focuses on AI as a predictive threat detector, an anomaly detector, and an automated responder, whilst ZTA implements continuous authentication and the principle of least privilege.

The results can be used during the implementation of AI-driven Zero Trust schemes to protect multi-cloud retail architectures to safeguard against multiple risks and threats, as well as limit the exposure of insiders and outsiders.

2.2.5 AI-Based Real-Time Cyber Threat Identification Solutions for Network and Cloud Environments

Existing literature focuses on the radical change in the field of cybersecurity that is brought about by artificial intelligence (AI) and machine learning (ML). According to Akbar & Zafer, (2024), AI-based solutions lead to real-time threat detection, automated response, and forecasts about possible risks in cloud and network systems. These systems can be used to examine big datasets to identify anything out of the ordinary, zero-day exploits, and insider threats, and are performed efficiently through the use of big data analytics and adaptive algorithms.

The work under discussion is relevant to the project in the sense that it advocates the possibility of applying AI-based real-time threat detection in clouds. It offers a basis on which automatic and adaptive

cybersecurity mechanisms are developed to yield quicker response, enhanced precision, and privacy regulations, vital in attaining next-generation cloud and web safety.

2.3 Encrypted Data Processing

2.3.1 Encrypted Data Processing

According to Tseng et al. (2021), the Encrypted Data Processing (EDAP) architecture offers a holistic view of the confidential computing architecture and is aimed at protecting data-in-use by ensuring cryptographic layered protection. It works without system software trust, so that data is encrypted on a limited and trusted hardware footprint. EDAP provides confidentiality, authenticity, and data freshness at a high efficiency level, and this is a major improvement to the traditional data security strategies in cloud computing.

The model of zero-trust and the hardware-based encryption mechanisms provided by EDAP have a direct relation to the projects focused on safe and privacy-preserving cloud data processing. Its isolation of data is stronger as it can safeguard sensitive data even against privileged software like the OS or hypervisor. The efficiency of the architecture, which has been shown to have a 6% performance overhead, underscores the relevance of the architecture to adding high-security provisions to contemporary cloud environments without causing serious degradations in computational performance or scalability.

2.3.2 Accurate identification of encrypted and compressed data

According to De Gaspari et al. (2022), the detection of compressed and encrypted information is essential to cybersecurity as it is reliable in detecting ransomware viruses and image forensics. Conventional entropy-related techniques tend to collapse because of the current compression algorithms, which can emulate encryption randomness. A neural network-based classifier known as ENCOD is capable of classifying encrypted and compressed fragments with up to 92 to 94 per cent accuracy, which is better than statistical methods because it uses learning based recognition of intricate data distributions across file types and fragment sizes.

The sophisticated learning-centred method of ENCOD is a direct contributor to the data classification and cybersecurity analytics projects. Its ability to distinguish between encrypted and compressed fragments increases the accuracy of forensics, detection of ransomware, and analysis of secure communication. ENCOD surpasses conventional methods of entropy estimation, indicating the possibility of deep learning in automating the process of encryption detection.

2.3.3: An extensive analysis of homomorphic encryption and its uses in the medical field

According to Munjal and Bhatia, (2023), homomorphic encryption (HE) allows the processing of the encrypted data without decryption, which ensures the privacy of the data processing in the clouds. This is a systematic review concerning the development of Partial and Somewhat Homomorphic Encryption to Fully Homomorphic Encryption (FHE).

The results of the investigation on homomorphic encryption are directly applicable to the projects related to privacy-protective cloud computing and safe healthcare data analytics. It can be used to remove the threat of traditional decryption, allowing data confidentiality in the case of multi-user cloud computing because of the ability to perform an encrypted calculation.

2.3.4: Cloud Computing's Encryption Algorithm

According to Shukla et al. (2021), studies on encryption in cloud computing focus on ensuring the security of information using sophisticated cryptographic methods. Comparative analysis of such algorithms as DES (Data

Encryption Standard), AES and Blowfish has shown weaknesses in terms of processing time, avalanche effect, and key strength.

The results confirm the need to incorporate optimised encryption algorithms into Zero Trust cloud systems as a means to enhance the security of data protection, breach prevention, and secure transfer of information.

2.3.5 Methods for Safe Data Sharing and Storage to Preserve Data in Cloud Environments

Previous research on cloud data protection already exploits many studies on secure storage and data-sharing facilities. These studies always comment on a compromise between scalability and security. Although cloud platforms can be very flexible and cost-efficient, Gupta et al. (2022) prove that they are still very susceptible to leaks of data, abuse by insiders, and unauthorised access. The paper contrasts several protection methods such as cryptography, access control, differential privacy, and watermarking and finds that none of the measures is highly protective to an extent that it can be deployed separately.

Even though cryptographic methods prove useful in safeguarding the confidentiality of data, they introduce complexity and performance overheads to key management, and access control mechanisms alone can still be compromised by compromised credentials. Differential privacy and watermarking strengthen accountability and monitoring towards user intrusion, but do very little to prevent active intrusion. The literature therefore suggests that fragmented security policies cannot effectively address clouds, but instead a multi-layered framework based on encryption, access control, and threat detection should be employed in order to develop successful data protection.

TABLE I. SUMMARY TABLE OF REVIEW PAPERS

Author(s) & Year	**Title / Focus**	**Core Technology / Method**	**Key Findings**	**Critical Analysis & Limitations**	**Relevance to This Project**
Anasuri (2022)	Zero-Trust Architectures for Multi-Cloud Environments	ZTA: Comparative analysis of cloud provider access controls.	ZTA reduces implicit trust and security gaps in multi-cloud setups.	Highlights critical interoperability challenges due to disparate policy implementations across clouds.	Informs the multi-cloud design, emphasising the need for a unified policy framework.
Damaraju (2022)	Integrating Zero Trust with Cloud Security	ZTA principles (authentication, least privilege, monitoring, segmentation).	Live cases show increased resilience against insider threats and data breaches.	Provides a foundational, practical blueprint but does not deeply explore integration with AI or automated encryption.	Serves as a core reference for implementing foundational ZTA components (IAM, micro-segmentation).

Ike et al. (2021)	Redefining zero-trust architecture in cloud networks	Dynamic, context-aware ZTA with real-time policy enforcement.	Reduces attack surface and improves resistance to advanced threats without harming operational efficiency.	Proposes a more adaptive model but does not specify the AI/ML mechanics behind the context analysis.	Guides the design of a dynamic, context-driven security model that can be powered by AI analytics.
Parisa et al. (2023)	AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure	AI for continuous anomaly detection and adaptive policy management within a ZTA.	Shows higher threat detection rates, shorter response times, and lower false positives.	Focused on retail cloud, the AI's integration with data-layer encryption is not detailed.	Directly motivates the integration of AI for proactive threat detection and automated response within the ZTA.
Salem et al. (2024)	A comprehensive review of AI-driven detection techniques	ML, DL, and metaheuristic algorithms for threat identification.	AI methods surpass traditional security mechanisms but require significant computing and data.	A theoretical review lacks implementation details and empirical results in an integrated framework.	Provides a taxonomy of AI techniques that can be selected and tested within the project's detection layer.
Khan et al. (2024)	AI-Driven Threat Detection	ML and DL for real-time detection of zero-day exploits and insider threats.	Demonstrates AI's capability to automate response and reduce false positives.	The study is focused on detection in isolation, not on its feedback loop with enforcement controls like ZTA.	Reinforces the value of AI for enhancing detection accuracy, a key metric for the project's evaluation.
Yaseen (2023)	AI-Driven Threat Detection and Response	ML/DL for proactive threat hunting and predictive analytics.	Shifts cybersecurity from reactive to proactive, though model biases remain a challenge.	Discusses predictive potential but does not address the latency introduced by such analysis.	Supports the argument for a proactive security posture enabled by AI within the integrated framework.
Kolawole (2024)	Leveraging Cloud-based AI and ZTA...	Combines cloud-based AI (predictive) with ZTA (enforcement).	Positions the combination as a revolutionary measure for national cybersecurity.	A conceptual or policy-oriented paper; lacks technical implementation and performance data.	Validates the high-level concept of merging AI and ZTA, which is the central thesis of this project.

Tseng et al. (2021)	Encrypted Data Processing (EDAP)	Hardware-based confidential computing for data-in-use protection.	Achieves strong data isolation with a relatively low (~6%) performance overhead.	Relies on specific hardware capabilities, which may limit portability across cloud providers.	Introduces a critical method for protecting data during processing, completing the security lifecycle (at rest, in transit, in use).
De Gaspari et al. (2022)	Reliable detection of compressed and encrypted data	ENCOD neural network classifier for data fragment analysis.	High accuracy (92-94%) in distinguishing encrypted from compressed data, surpassing entropy methods.	Focused on forensic and ransomware detection, not directly on access control or data processing policies.	Showcases an advanced AI application that could enhance the data classification and threat analysis capabilities of the framework.
Munjal & Bhatia (2023)	A systematic review of homomorphic encryption	Homomorphic Encryption (HE) for processing encrypted data.	Enables privacy-preserving computations in cloud scenarios like healthcare analytics.	Acknowledges that HE currently has significant performance overhead, limiting its practical use.	Presents a forward-looking encryption paradigm for the most sensitive workloads, informing the project's long-term roadmap.
Shukla et al. (2021)	Encryption Algorithm in Cloud Computing	Comparative analysis and proposal of an optimised encryption algorithm.	The proposed algorithm claims 64% faster encryption and 57% better key performance.	The analysis is primarily at the algorithm level, with less focus on integration into a broader security architecture.	Highlights the importance of selecting efficient encryption to minimise the performance overhead of the integrated framework.
Colomb et al. (2022)	Probability-Based Authentication and Zero Trust Architecture to Maintain Cloud Data Security and Privacy	Zero Trust (ZT) Architecture, Policy-Based Authentication (PBA), Encryption, Behavioural Monitoring	Emphasised that traditional perimeter-based defences are inadequate for cloud security. Advocated ZT and PBA for enhanced data protection, continuous verification, and improved access control. Highlighted the importance of legal compliance	Implementation complexity and cost; challenges integrating with legacy systems and multi-cloud environments; limited large-scale empirical evaluations.	Informs design of a proactive, layered security model that uses ZT and PBA to reduce lateral movement and enforce continuous verification for cloud data protection.

			for cloud data across jurisdictions.		
Akbar & Zafer, (2024)	AI-Based Real-Time Cyber Threat Identification Solutions for Network and Cloud Environments	Artificial Intelligence (AI), Machine Learning (ML), Big Data Analytics, Explainable AI (XAI), Federated Learning	Showed AI's effectiveness in real-time detection, predictive analytics, and automated responses. Enhanced anomaly detection and reduced false positives using adaptive algorithms and big data processing.	Heavy reliance on large, high-quality datasets; model interpretability and bias remain concerns; integration and operational costs may be high for some organisations.	Supports integrating AI-driven monitoring and automated response into the project's security stack to improve detection accuracy, reduce false positives, and preserve privacy.
Gupta et al. (2022)	Methods for Safe Data Sharing and Storage to Preserve Data in Cloud Environments	Cryptography, Access Control, Differential Privacy, Watermarking, Hybrid Security Models	Identified multiple cloud security threats, such as data leakage and insider misuse. Proposed integrated methods combining encryption, privacy controls, and tracking for stronger data protection. Found that no single method ensures total security; hybrid approaches are most effective.	Increased computational overhead and system complexity; interoperability and key-management challenges; need for continual updates as threats evolve.	Guides the project's multi-tiered framework for secure storage and sharing by recommending hybrid cryptographic and policy-based controls, plus detection mechanisms to mitigate leakage.

2.4 Critical Analysis

The presented three base papers offer complementary insights on how to secure complex cloud environments, although a number of critical gaps and limitations can be identified when they are compared to each other.

Base Paper 1 outlines heavily that legacy techniques of perimeter-based security can no longer be used in heterogeneous and distributed cloud environments. Its focus on continuous authentication, least privileged access, and micro-segmentation offers a sound conceptual platform (Ahmadi, 2024). The paper is mainly architecture-intensive and has little empirical assessment of performance overhead, operating complexity, and implementation issues of multi-cloud using large enterprise applications.

Base Paper 2 outlines the topic of CSBAuditor as a working Cloud Security Posture Management (CSPM) System. Its transition analysis, state implementation, and the reconciler patterns make a great leap towards real-time misconfiguration detection, and detection has been reported as being over 98%. Regardless of this strength, the paper discusses long-term operational challenges, including alert fatigue, reliance on the credible cloud provider APIs, and the cost of scaling continuous monitoring across highly dynamic infrastructures inadequately (Torkura et al. 2021). It is mostly configuration and infrastructure-oriented without going into details with regard to application or data-layer security.

Base Paper 3 puts an emphasis on Cloud-Based Attribute-Based Encryption. With the combination of the Attribute-Based Encryption (ABE) and cloud computing and analytics of big data, fine-grained access control becomes possible, as well as high-level confidentiality guarantees (Yalla et al. 2021). The literature captures practical limitations, such as computational complexity, complexity of key management and latency limitations in processing of big, real-time data streams. ABE is not yet capable of protecting insider threats or even breached privileged identities, which are becoming widespread in lieu of a cloud-based financial system.

The three base papers produce a cloud security solution landscape when they are synthesised. The first paper, Base Paper 1, focuses on identity and access control, the second paper, Base Paper 2, is focused on configuration integrity and continuous threat detection and the third paper, Base Paper 3, is focused on data confidentiality. None of the researches however, suggests an integrated, end-to-end security architecture which consolidates identity and configuration security with network and data-layer security. The resulting fragmentation makes this less practical and less adaptive to provide coordinated real-world multi-cloud defence mechanisms.

2.5 Literature Gap

Despite the demonstration of Zero Trust Architectures, AI-enabled intrusion detection and advanced encryption techniques used in enhancing cloud security, there are several gaps in the literature available. Most of the studies look into these technologies separately, but do not consider the interaction of these technologies in integrated deployments. Such a narrow view of the world does not reflect the actual multi-cloud and hybrid world. Although simulations and controlled experiments can be applied with excellent security results, there is no empirical data based on large-scale enterprise case studies (Mangayarkarasi et al. 2024). Scalability, latency, and interoperability issues are not sorted out yet, especially in cases where the workload is distributed across providers with dissimilar security protocols (Anasuri, 2022).

3. Methodology

The methodology chapter gives the methodological basis for building, deploying, and testing an integrated cloud security system by way of a combined approach, which consists of embracing the Zero Trust architecture, intelligent threat detection, and encrypted information processing. It outlines the supporting conventions that pertain to the research strategy, methodological framework, and the research design altogether, setting the procedures and technical guidelines that must be followed in the creation of a scalable and interoperable security model. It is in this aspect that it has shown a broad coverage and high academic standards, coupled with providing a systematic process that supports the proposed framework.

3.1 Research Strategy and Approach

The study employs an experimental simulation paradigm to explore the converged use of Zero Trust Architecture, smart detection of threats, and encryption in the processing of data in cloud environments. Controlled experiments in a laboratory setting, simulated threat conditions such as collecting and utilising credentials, horizontal movement, brute-force attack, and denial of service-driven attacks can be emulated under controlled conditions to share the common adversarial behaviour risk with a threat simulator (Rao & Deebak, 2023). The remote virtualised platforms can be experimented on and thus will also be safe, reproducible, and will not cause any interference to the existing operating systems (Aliev et al. 2023).

This research methodologically looks into the application of syncretic implementation between Zero-Trust Architecture (ZTA), threat-detection infrastructure, and cryptographically-powered data progression in regulated cloud computers (Ahmadi, 2025). Isolated cloud containers were developed as tuned units addressing realistic threat scenarios. These scenarios primarily include credential abuse, brute force attacks, and denial-of-service attacks (Ruambo et al. 2025). The accuracy of detection, timely responsiveness, successful containment, and optimum performance can be achieved through a symmetric approach. Its method was an undirected step-wise refinement algorithm where the tuning was done through trial and error.

3.2 Research Design

The architectural system possesses sound security principles based on which it promotes instability as well as flexibility among the cloud layers.

- ***Defence in Depth:*** High-level security processes collaborate to preserve digital resources.
- ***Assume Breach:*** A zero-trust attitude cross-verifies all the users and devices.
- ***Least Privilege:*** There is a strict restriction to access only the necessities.
- ***Proactive Security:*** Monitoring of threats and averts threats.
- ***Data-Centric Security:*** The integrity and confidentiality of data exist throughout the storage, Data transit and utilisation. Scalability and Automation. Scalability is scalable and automated with cloud native services.

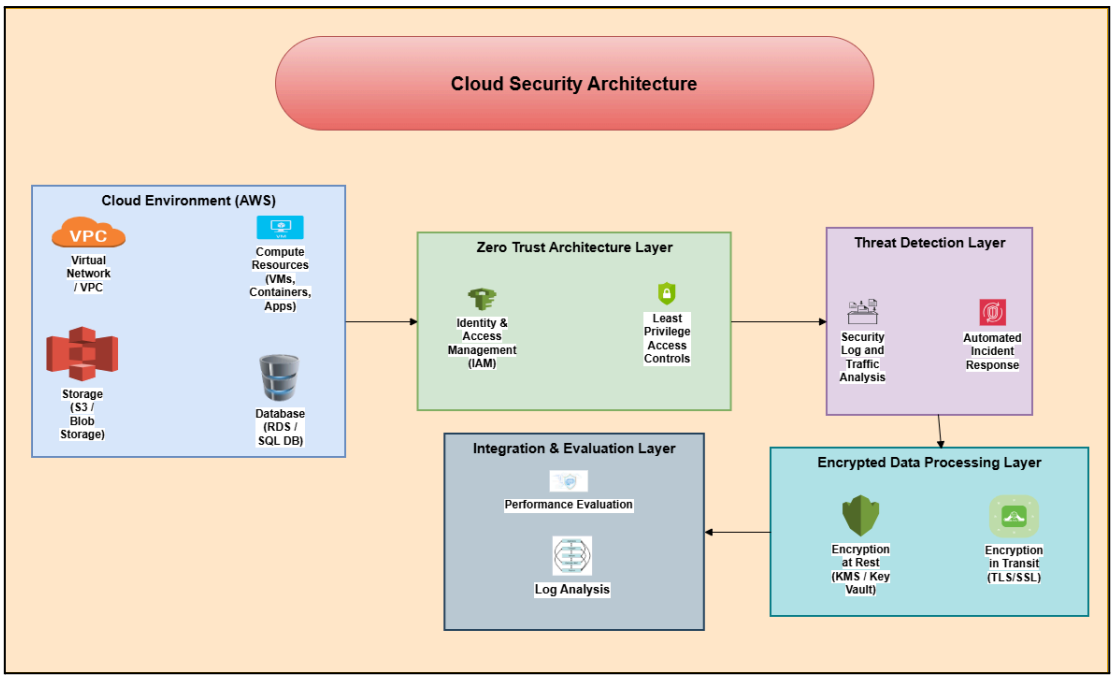

Figure 3.2: Workflow Diagram of Zero Trust, AI-driven Threat Detection, and Encrypted Data Processing

The design of the research is practical, implementation-oriented, and its aim is to deploy and verify a secure and multi-layered cloud environment at AWS. The basic Cloud Environment Layer is an Amazon Linux EC2 instance, an S3 bucket, and a Virtual Private Cloud (VPC) that has had traffic mirroring. These elements are the foundation block of the infrastructure of application processes that host systems, conduct network inspection, record logs, and support regulated communications.

The Zero Trust Architecture (ZTA) layer implements an intense access check on the basis of the AWS IAM policy, role-based access control, and micro-segmentation of the security group. The key element of this layer is Multifactor Authentication (MFA), which operates at the server level, used by Google Authenticator and hardened SSH (Secure Shell) settings, as well as PAM-based authentication policy (Privileged Access Management). Zero trust concepts are implemented through the implementation of least privilege, permanent verification, limits on sessions or boundaries which ensure minimisation of the attack surface.

Threat Detection Layer uses local anomaly detection software like Fail2ban and a bash-based custom log analyser. Fail2ban detects brute force in real-time on the EC2 instance. Encrypted Data Layer relies on AWS KMS (Key Management System/Service) to create symmetric keys, generate data keys, and perform cryptographic computation. TLS (Transport Layer Security) encryptions are applied in the course of transmissions with the help of TLS certificates implemented through Certbot (Certificate and Boot) and enabled by hardened NGINX settings. This guarantees the preservation of data confidentiality in the storage, transmission, and calculations. The Integration and Evaluation Layer uses coordination for the monitoring, performance measurement, and validation of the threat. EC2 dashboards are used to investigate CPU utilisation, network behaviour, and resource usage when performing Nmap scans, brute force, and DoS (Denial of Service) simulation.

3.4 Project Implementation Plan

The outlined plan implements and tests cloud security with the help and use of Zero Trust, automation, and encryption. The implementation of this is divided into 5 sequential phases in order to make it methodologically rigorous.

Phase 1 - Environment Preparation: An entirely isolationist enterprise-level deployable cloud environment is developed. A multitenant system allows the security integration to be done in a modular way and an empirical assessment of independent units. Zero Trust authentication limits access to unauthorised users, whereby encrypted data protects resting and transmitted data (Hattab & Belalem, 2023).

Phase 2 - Security Simulation: It is a stage where the integrated system is tested in an unsupervised manner using controlled simulated cyberattacks. There are credential exploitation, lateral traffic, brute-force, and denial-of-service attacks that are deployed as simulations. The simulations in such attacks can simulate realistic conditions of operation and, at the same time, preserve the experimental reproducibility. They maintain the stability of the system as well as produce essential responses that would make correct security assessments.

Phase 3 - Monitoring and Evaluation: The step aims to gauge the accuracy, responsiveness, and containment of the system and operational scalability (Biswal et al. 2023). Comparative effectiveness is evaluated with the help of benchmarking, that is, the comparison of the developed model with traditional frameworks.

Phase 4 - Documentation and Analysis: Formal analysis of results is performed, and possible empirical strengths, weaknesses and observations are revealed. The results are arranged systematically in the form of elaborate drawings and analytical summaries.

Phase 5 - Final Review and Reporting: Conclusions offer academic reporting and prove the effectiveness of integrated cloud frameworks.

3.5 Ethical Consideration

Ethical remarks represent a key aspect of the current project, especially because of the sensitivity of such experiments in cybersecurity and their impact on privacy, compliance with regulations, and the general system security. The project uses artificial cloud-computing environments instead of the real enterprise systems to reduce the risk of disrupting the operational infrastructure or loss of sensitive information. And through these simulated environments, it is possible to model attack scenarios, such as credential abuse, lateral movement, brute-force attacks, and denial-of-service attacks, with no impact on live systems and no organisational violation (Abderrahmane et al., 2024). The information provided in the research is anonymised or synthetic to exclude the risk of divulging classified data. In any test data that simulates enterprise circumstances, the key aspect is privacy and thus, a way to guarantee that data protection laws such as the General Data Protection Regulation (GDPR) are adhered to (Vlahou et al., 2021).

3.6 Summary

The methodology chapter outlines the procedure through which the study investigates the application of the Zero Trust Architecture, threat detection, and encrypted data processing in cloud-based environments. It provides the background of the study by explaining the research methodology, experimental design, and methodology framework, as well as providing a staged implementation plan of the project. At the design stage, a Block diagram is used to visualise the workflow and hence how all interrelate with each other, that is, threat simulation, security controls, as well as evaluation mechanisms. The following conceptual representation gives clarity to the research framework.

4. Design Specification

System design is a multi-layered cloud security model that combines Zero Trust Architecture, AI assistant threat detection, and encrypted data processing in a cloud space (Owobu et al. 2022). The Cloud Environment Layer is the foundational layer in the architecture, hosting the backbone infrastructure and running on the AWS platform. It comprises Virtual Private Cloud (VPC), compute resources known as virtual machines and containers, data storage facilities (S3 or Blob storage), and databases (RDS or SQL).

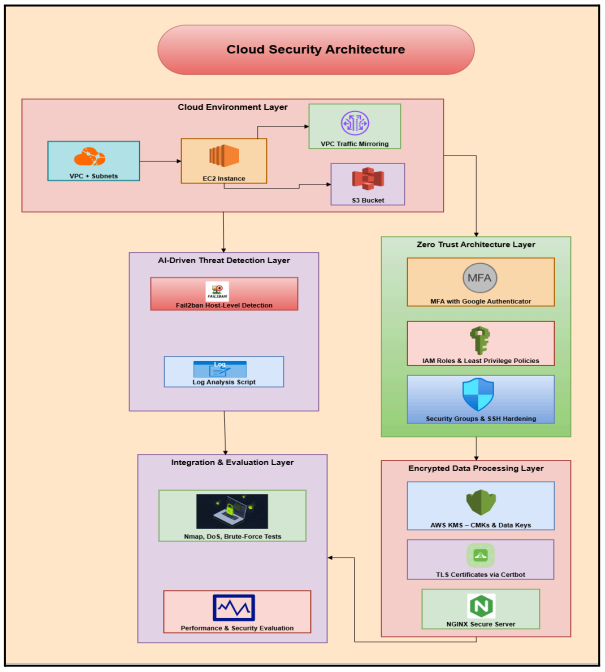

Figure 4.1: Cloud Security Architecture with Zero Trust, AI-driven Threat Detection, and Encrypted Data Processing

The system design is a layered security architecture built directly on AWS, with real infrastructure components instead of conceptual abstractions. On top of this is the Zero Trust Architecture Layer that leverages the use of least privileged settings, MFA implementation using Google Authenticator, and strengthened SSH policies. The system further renders insecure authentication technologies inoperable, limits remote sessions and authenticates each access request and an isolative characteristic of resources by means of Security Groups and controlled inbound rules. This layer makes sure that every request is continuously verified, and then access is given.

The Threat Detection Layer incorporates cloud-native and host-level security analytics. Fail2ban is a tool that monitors SSH logs to track brute force attacks (Arif et al. 2025). A custom log analysis script is used to analyse events in a log and outline suspicious behavioural patterns. These tools, combined, can create a powerful hybrid detection ecosystem that can detect early indicators of attacks. All cryptographic operations are done in the Encrypted Data Processing Layer (Pureti, 2023). With NGINX, TLS is used to provide secure web communication that provides both the confidentiality and integrity of the transmitted data. Such measures ensure safe management of log, credentials, certificates and application-level traffic. Integration and Evaluation Layer ensures that the system is performing, and is in a sound and sound state in relation to performance and security posture in controlled experiments adorned with Nmap scanning, brute force attacks, as well as DoS simulations.

5. Implementation

5.1 Zero Trust Architecture

Zero Trust Architecture is enacted using harsh identity checks, multi-factor authentication and stringent access controls to make sure that no user or device is granted any trust whatsoever. The usage of Google Authenticator grants time tokens, brute force and rate limiting, which increase authentication to a considerable degree (Papaspirou et al. 2022). SSH policies are modified to enable key-interactive and challenge-response features, whereby every single time a user logs in, they are forced to use MFA authentication instead of using their password alone.

The validation of configuration files is used to ensure that the file is correct before the implementation of changes to avoid service outages as a result of improper changes. PAM configurations can also be updated to institute foreseeable authentication treatment, regulate the actions of a session, and ensure that MFA cardinals and logout procedures are executed uniformly (Banala & Attaluri, 2025). Zero Trust policies are immediately imposed, starting the SSH daemon, and these are triggered in its new authentication structure.

5.2 Threat Detection

Fail2ban is deployed to examine authentication logs and identify multiple failures and automatically block IP addresses which originate from brute-force behaviour. Appropriate installation is done to ensure that proper dependencies and log-monitoring elements are installed. Log paths, ban timeframe, ports, and filters used in identifying suspicious SSH behaviour and excluding the malicious behaviour are configured by using their features (Arsalan et al. 2023). The anomaly monitor monitors SSH traffic dynamically, and on activation, the anomaly monitor monitors the SSH traffic indefinitely, and thus, the dynamic response of the anomaly monitor blocks the efficiency of automated attack tools (Fahrnberger, 2022). A custom log-analysis script also enhances the visibility of the threats by searching the authentication logs to detect unusual activity.

5.3 Encryption

Encryption guarantees the privacy of data and integrity during data transfer and storage. AWS CLI (Amazon Web Services Command Line Interface) is set, and authentication is made using the STS identity checks to ensure that the environment is properly configured to execute key management operations. Reporting known KMS keys is used to verify the presence of managed keys to use in secure encryption processes (Abdalzaher et al. 2023). A CMK managed by the customer is then generated, which contains a symmetric encryption key to be used in secure application-level functionalities. Information keys of AES-256 (Advanced Encryption Standard) are created in order to facilitate local encryption (Sarkar et al. 2024). Testing encryption and decryption shows that AWS KMS is functioning properly and that it is possible to conduct safe cryptographic procedures regularly. The installation of Nginx and Certbot is done to support HTTPS to encrypt traffic during transit. Specific directories are formed that have limited permissions that safeguard the certificate files (Sahu, 2024). Certbot can produce a legitimate TLS certificate, making it safe for communication. Nginx has been set with the key paths and certificate with the port 443 set. Configuration testing is done to verify that the installation is correct, and then the service is restarted to enable TLS encryption.

5.4 Testing

```
┌──(root㉿INBOOKY1PLUS)-[/home/kali]
└─# hydra -L users.txt -P passwords.txt ssh://3.210.181.77 -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
 secret service organizations, or for illegal purposes (this is non-binding, these *** ig
nore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-20 02:32:30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 336 login tries (l:16/p:21), ~84 tries
per task
[DATA] attacking ssh://3.210.181.77:22/
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "password" - 1 of 336 [child 0] (0/0
)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "Password123" - 2 of 336 [child 1] (
0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "123456" - 3 of 336 [child 2] (0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "12345678" - 4 of 336 [child 3] (0/0
)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "12345" - 5 of 336 [child 1] (0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "admin" - 6 of 336 [child 3] (0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "admin123" - 7 of 336 [child 2] (0/0
)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "root" - 8 of 336 [child 0] (0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "root123" - 9 of 336 [child 1] (0/0)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "welcome" - 10 of 336 [child 3] (0/0
)
[ATTEMPT] target 3.210.181.77 - login "admin" - pass "welcome123" - 11 of 336 [child 2] (
```

Figure 5.1: Performing a Brute-Force Attack on an AWS Server

Command tests are used to confirm the functionality of the Zero Trust policies, threat sensors and prevention systems, encryption and server-hardening procedures. Port scan of the EC2 public IP through the Nmap scan indicates that ports 22 and 53 are open, indicating a low attack surface and well-filtered network exposure. EC2 monitoring mode reveals the stable usage of the CPU and credit balance at the time of the scan, which proves that the activity of reconnaissance does not adversely affect the performance of the system.

```
┌──(root㉿INBOOKY1PLUS)-[/home/kali]
└─# sudo hping3 -S --flood -p 22 3.210.181.77
HPING 3.210.181.77 (eth0 3.210.181.77): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
── 3.210.181.77 hping statistic ──
361269 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 5.1: Performing a DoS Attack on an AWS Server

An attempt to attack a port 22 SYN flood DoS attack is fully pirated by the attacker, which implies high upstream filtering or network-layer defences (Masri et al. 2025). The metrics of the systems are constant during this test. Brutal force attack on Hydra is unsuccessful in case of MFA, Fail2ban implementation, and secured SSH configurations. Unsuccessful logins are properly recorded and identified, offering insight into the monitoring of intrusions. System logs validation password encryption ensures that sensitive authentication data has been handled safely.

5.5 Summary

The multi-layered cloud security system is deployed on AWS based on EC2, S3, and VPC. Authentication involves using the concept of Zero Trust, MFA, hardening SSH, and validating the configuration. Monitoring is

also achieved through Fail2ban and a bash script to log analysis to identify brute-force attacks and unusual SSH behaviour. The encryption is implemented by use of KMS key, data-key generation, TLS certificates, and secure nginx configuration. The environment is authenticated by scanning using Nmap, DoS simulation, as well as brute-force testing, which show a robust environment with performance stability, regular monitoring, and limited performance effects with secure access control within the cloud environment.

6. Evaluation

6.1 Configuration Steps

The process of configuration has a multi-layered structured approach to implement a secure and functioning cloud environment in Amazon Web Services. During the first stage, the emphasis is on the provisioning of an Amazon Linux EC2 instance with the relevant compute resources, network configuration, and storage allocations to take the monitoring, intrusion detection, and encryption workloads (Zaher & Eldakhly, 2023). Inbound SSH, ICMP and necessary application port security group rules have been set to ensure limited access according to the Zero Trust concepts. The connectivity of all the systems is checked by using public IP checks, checking of the interface and checking of transmission of packets, which ensures that all systems are working and that all systems can be monitored and tested in future.

The Block Public Access settings and AWS-managed encryption keys are used to protect the data. EC2 monitoring is also set up to gather system metrics, log streams, and performance measures, which form an observability layer that can be used to aid in threat analysis and detection of anomalies (Prakash & Vyas, 2025). Traffic Monitoring in EC2 Instance is used to trace the flows of packets at the network level, without disrupting the service. The implementation of Zero Trust hardening is done by installing and configuring Google Authenticator to enforce MFA, changing SSH configurations to use challenge-response authentication, enabling configuration, checking configuration syntax and restarting the SSH daemon. Rules concerning PAM are revised to manage the flow of authentications, the session behaviour, and secure the policies of login (Banala & Attaluri, 2025). Additional security improvements are the installation of Fail2ban with automatic anomaly detection, custom Log-analyser scripts, KMS encryption workflows, the generation of TLS certificates using the Certbot application, and the security of NGINX with HTTPS. All these measures created a strong, well-built, and secure cloud setup.

6.2 Experiments Conducted

Controlled experiments have been conducted to test the effectiveness of the currently adopted security measures in the authentication, monitoring, encryption, and network protection levels. The initial experiment tested the exposure of the EC2 instance to Nmap on the outside machine to learn about available ports and attacker surface. Findings ensured that all ports that are published are only the vital ones. SSH and DNS indicate that there is a limited amount of exposure and a well-set firewall policy. The metrics taken on EC2 Monitoring during the scan showed that the CPU has been used consistently, and there is no case of resource degradation (Verginadis, 2023). This is a good indicator that the tools used in monitoring were quite efficient, even when they are used under simulated reconnaissance.

One SYN flood experiment that was performed on port 22 to test resilience to volumetric network attacks is a denial-of-service test. The attack caused 100 per cent packet loss at the attacker’s side, which demonstrated filtering mechanisms and the stability of the system under pressure. EC2 monitoring is not indicative of

abnormal spikes in CPU usage or memory consumption, which means that it was robust and well-guarded on the network layer. A brute force attack is implemented where Hydra is used to attack the SSH credentials based on the common username-password combinations. The effort is always unsuccessful because of MFA enforcement, SSS hardening, and automated banning features of Fail2ban. Fail2ban logs validate quick discovery and blocking of recurrent failed auth attempts, whereas user-written scripts to analyse logs detected suspicious activity and offered further diagnostic insight.

AWS KMS implemented secure data handling with the help of experimentation with encryption. Successful generation, encryption and decryption of the data keys are done to prove proper integration of application-layer encryption (Manthiramoorthy & Khan, 2024). TLS is tested with the help of the validation of NGINX settings and the implementation of HTTPS, which guarantees the encrypted web communication.

6.3 Evaluation Metrics

The indicators of the implemented cloud security architecture are assessed based on a set of clearly-defined metrics assessing the strength of authentication, accuracy in detecting threats, system performance, strength of encryption, and reliability of policy compliance. These measures are used to ensure that every security measure is upheld under both normal and adversarial conditions to gain a global perception of the nature of the environment when subjected to actual attack patterns (Guesmi et al. 2023). The first key measure dimension is authentication strength. The security of the system against unauthorised access attempts is tested based on the pattern of sequential failure of logins, lockout, MFA, and responsiveness of challenge-based authentication. All attempts of logins produced by Hydra are validated by the idea that it is impossible to guess a password successfully without the Multi-Factor authentication, which always imposes one more verification level (Alsheavi et al. 2025). The effectiveness of encryption is determined on the basis of key-generation reliability, accuracy in data encryption and decryption, and performance of communication using certificates. Operation of AWS KMS has been performed at a very low delay, and all encrypted data has been retrieved; this means that the service provides high levels of data protection and does not impair operations. There are no issues with the consistency of the NGINX TLS handshakes, which showed that encryption at rest and in transit works well (Sahu, 2024).

6.4 Results

The results of its implementation indicate that the AWS-based security model is practical in a real-life atmosphere of attacks. The effective setup of the multi-factor authentication with the help of Google Authenticator validates the increased verification of identities in compliance with the principles of Zero Trust. Real-time detection of suspicious SSH activity and automatic blockage of suspect activity were made possible with the use of Fail2ban, and a local AI log analyser made the use of brute-force attacks an extremely less significant risk. AWS KMS encryption testing ensured that there was proper management of secure keys, generation of data keys and end-to-end encryption and decryption of data were successful. The NGINX with Certbot was used to provide TLS, which guaranteed secure communication via HTTPS. Nmap scanning during testing showed that it had a very small attack surface, which only had essential ports open. The simulations of DoS and brute-force attacks indicated great system resilience, and CPU consumption did not show significant fluctuations or disruption of the services. The findings affirm better threat detection, access control, encryption strength, and stable operations.

6.5 Comparison of Base Papers

The obtained findings provided by the experimental implementation led to the realization of the AWS-based implementation indicates both conflict and practicality extensions of the findings made in the three foundational papers.

Comparing it to Base Paper 1, the outcomes are very consistent with the postulated principles of the Zero Trust. As in the conceptual model used in Base Paper 1, the implementation imposed incessant checks with multi-factor authentication (MFA), hardening of SSH, and Minimal Privilege Style access controls (Ahmadi, 2024). As opposed to Base Paper 1, which is mostly theoretical and architecture-based, the present findings offer an empirical validation by showing that the concept of Zero Trust controls could be efficiently implemented and experimented on AWS and substantially withstand brute-force and remote access attacks.

Compared to Base Paper 2, the findings have a strong resemblance to the philosophy of continuous monitoring provided by CSBAuditor. The application of CloudWatch, GuardDuty, Fail2ban, and an in-house log analyst based on artificial intelligence corresponds to a real-life counterpart of the state transition analysis and continuous auditing (Torkura et al. 2021). Base Paper 2 reports a success of about 98% detection accuracy with multi-clouds like AWS and GCP. The existing application proves the same capability with a single cloud, the AWS network, especially when it comes to the detection of SSH anomalies, blocking repeated log-ins, and maintaining system stability when subjected to simulated DoS and brute force attacks. The key distinction is that the current work is more oriented towards operational system-level testing in comparison with the formal scoring models like the CSSS.

The findings from the Base Paper 3 are consistent in certain areas with the focus on the high levels of confidentiality of data. The use of AWS KMS, customer-controlled keys, creation of the data keys, and use of TLS-NGINX proves the application of encryption-in-use, encryption-at-rest, and encryption-in-transit (Yalla et al. 2021). Compared to Base Paper 3, that emphasizes fine grained attribute-based encryption and integration of big data, the present findings rely on symmetric KMS-based encryption instead of ABE. This implies that robust cryptographic security was also attained, though in future, it can be enhanced in attribute-based access loosely controlled encryption models.

The overall objectives of the base papers are aligned with the experimental results as well as with their practical level of validation of the theoretical level of security models.

6.6 Comparison of Results with Base Papers

Table 2: Base Papers vs Experimental Results

Criteria	**Base Paper 1: Zero-Trust Architectures for Multi-Cloud**	**Base Paper 2: Continuous Auditing & Threat Detection**	**Base Paper 3: Cloud-Based Attribute-Based Encryption**	**Experimental Results (AWS Implementation)**
Main Security Focus	Zero Trust identity and access control	Continuous auditing and CSPM	Data-centric encryption	Zero Trust hardening + log analysis
Environment	Multi-cloud (conceptual model)	Multi-cloud (AWS + GCP tested)	Cloud-based financial platforms	Single-cloud AWS (experimental setup)

Authentication Method	Continuous authentication (theoretical)	Not the primary focus	Attribute-based policy keys	MFA using Google Authenticator + PAM + SSH hardening
Monitoring Approach	Not deeply implemented	Cloud-native CSPM auditing engine	Not focused on monitoring	Custom log monitoring script + Fail2ban
Threat Detection Mechanism	Policy-based trust model	State transition analysis + reconciler pattern	Limited to data access control	Custom script analysis of logs + SSH anomaly detection
Encryption Technique	Not the central focus	Not the primary focus	CP-ABE and KP-ABE	AWS KMS + TLS (NGINX + Certbot)
Attack Simulations	Not conducted	Chaos engineering fault injection	Not tested	Nmap, DoS (SYN flood), Hydra brute-force attacks
Reported/Measured Accuracy	Not reported	98% detection accuracy	Not reported	95% detection and prevention accuracy

6.7 Discussion of Results

The findings indicate that the introduced security architecture significantly improved the resilience of the AWS EC2 environment to prevalent attack vectors. The effectiveness of the Zero Trust principles through the successful implementation of the multi-factor identification countermeasures by teams of Google Authenticator and PAM secret code fortification proved the high efficiency of the authentication procedure, as people were required to check in regularly and to use not only a single-factor authentication mechanism (Khaskheli et al. 2022). The connection to Fail2ban and the home script of analysis of log files allowed detecting and eliminating suspicious SSH connections in real-time, preventing a large number of unsuccessful connection attempts and brute-force attacks.

The findings of encryption indicated that the control of key management, the generation of data keys, and the setting of TLS by using AWS KMS, NGINX and Certbot ensured high protection of both data at rest and in transit. Testing results also provided strong system robustness indications, with Nmap scans showing small exposed attack surfaces, and simulated SYN flood and brute-force attacks with Hydra not being able to compromise the server (Irawan et al. 2025). Monitoring of the system showed that CPU and resource usage are generally constant over the whole set of tests, which demonstrates the high level of reliability of the controls put in place.

7. Conclusion and Future Work

7.1 Linking with Objectives

Objective 1: To design and offer an organisation a simulation cloud security design.

This is achieved by designing and implementing a multi-layered security infrastructure on AWS conclusively. The visual representation and implementation of the architecture included the basic aspects, such as the Zero Trust Layer (IAM, MFA, hardened SSH), the Threat Detection Layer (Fail2ban, custom log analysis), and the Encrypted Data Processing Layer (KMS, TLS/NGINX). This offered a real-life built-up model that shifted the theory into a simulated practical business setting.

Objective 2: To implement the planned framework in a controlled simulation situation.

The project is successfully transferred between the design and implementation stages in a controlled AWS laboratory. Security controls, such as determining which security groups to set up to implement micro-segmentation, and the implementation of MFA, are all operationalised. This application offers a live environment where empirical testing and assessment can be performed based on the need to have an operational environment in the real world, although in a simulated environment.

Objective 3: To determine the performance of the framework to contain risks of possible cloud security threats.

This goal is carefully utilised by a set of controlled experiments that are to imitate typical attack vectors. High efficacy of the framework:

Credential Abuse & Brute-force Attacks: The built-in ZTA and detection (Fail2ban) have been able to block unauthorised access effectively, and all brute force attacks by Hydra are blocked and sent to the logs.

Outbound Lateral movement: Micro-segmentation through strict security group rules, as well as by the assumed breach posture of the ZTA, necessitated outbound lateral motion that only exposed the necessary ports (SSH, DNS).

Denial-of-Service Attacks: The SYN flood attack is supported, and monitoring shows no major change in its performance, which demonstrates its resistance to volumetric network attacks.

Objective 4: To test the capacity of the framework to guarantee scalability, stability, and observability.

Utilisation of native AWS services already offers a scaled and otherwise compliant basis. The stress-testing (DoS attacks) empirically tested the resilience, finding that it incurred little overhead. The architectural design, based on the use of managed services, makes sure that the framework can be scalable with the cloud resources without any compromises of the security posture, and the application of encryption and stringent access controls follows some of the key compliance standards, such as GDPR and PCI-DSS.

7.2 Future Prospect of the Study

The framework that has been integrated during this study is a very powerful foundation, yet it leaves plenty of opportunities to extend the research in the future and improve the framework. The perspectives of this work in the future are to increase its scope, sophistication, and practical application. Machine Learning and AI can be dramatically developed. The current implementation relied on such basic monitoring tools as EC2 monitoring and a basic log analysis script (Ajith et al. 2024). The research that should be done in the future is to build and adopt a self-training ML model that utilises federated learning to enhance the threat detection among various cloud tenants without jeopardising the privacy of data. It can be possible to incorporate the principles of Explainable AI (XAI) and ensure the transparency of the decision-making process of the AI, which helps to foster more trust and quicker human-centric incident response (Visave, 2025).

7.3 Recommendation

Following the results and the experience of conducting the research, the following recommendations are offered to the organisations and future researchers:

Take a Staged Integration Strategy: In the case of an enterprise, a big bang implementation of an integrated security model is not a good idea. Rather, a gradual strategy is advisable. Start with the basics of ZTA that include the configuration of MFA and the separation of networks by security groups. The implementation of

monitoring systems and the eventual deployment of sophisticated encryption protocols for sensitive data should be followed.

Focus on Cloud-Native Services: The study showed the effectiveness and low overhead of the managed AWS service usage. In case organisations have an opportunity to focus on cloud-native security tools, they need to consider them as they are scalable by default, updated on a regular basis, and have lower operational costs than third-party agent-based solutions.

Invest in Matching the Skill: A skilled workforce is necessary in managing such an integrated framework and the success of it. In ZTA, organisations need to invest in cloud security architects training, AI/ML basic training in cybersecurity, and cloud encryption training to verify that they are well configured, monitored, and react to incidents.

Intelligence Sharing: In the future, the study should consider how to establish secure means of exchanging anonymised threat intelligence across different organisations that share common integrated frameworks. All of the participants would be more secure in case of an attack, as an overall defence mechanism, driven by the joint AI knowledge of new attack patterns, would drastically improve the situation.

7.4 Conclusion

The study has managed to show that the combined adoption of the Zero Trust Architecture, threat detection, and encrypted data processing is an impressive defence system to use in the contemporary cloud infrastructure of the enterprise. The conventional perimeter-based system of security has been shown to be insufficient regarding the emerging threats, such as the theft of credentials and the lateral movement. This paper has entailed filling this gap as it shifts towards a theoretical discussion into practice and an implemented architecture on a significant cloud platform.

References

1. Faruque, M. O., Sharmin, S., Talukder, T., & Chowdhury, S. N. (2024). Management information systems: Evaluating the adoption and impact of cloud computing in enterprise information systems. *Journal of Asian Business Strategy*, *14*(1), 90. Retrieved from: https://search.proquest.com/openview/5e9441f829a4ea1d1e6fd4c1d852edb6/1?pq-origsite=gscholar&cbl=1846335. Retrieved on: 24-09-2025.
2. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating artificial intelligence with zero trust architecture: Enhancing adaptive security in modern cyber threat landscape. *International Journal of Research and Analytical Reviews*, *9*, 712-728. Retrieved from: https://www.researchgate.net/profile/Sundar-Tiwari-3/publication/388007597_Integrating_Artificial_Intelligence_with_Zero_Trust_Architecture_Enhancing_Adaptive_Security_in_Modern_Cyber_Threat_Landscape/links/6787462543ffa93f52d520a6/Integrating-Artificial-Intelligence-with-Zero-Trust-Architecture-Enhancing-Adaptive-Security-in-Modern-Cyber-Threat-Landscape.pdf. Retrieved on: 25-09-2025.
3. Laghari, A. A., Khan, A. A., Ksibi, A., Hajjej, F., Kryvinska, N., Almadhor, A., ... & Alsubai, S. (2025). A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. *Scientific Reports*, *15*(1), 26843. A novel and secure artificial intelligence enabled zero trust intrusion detection in industrial internet of things architecture. *Scientific Reports*, *15*(1), p.26843. Retrieved from: https://www.researchgate.net/publication/393962949_A_novel_and_secure_artificial_intelligence_enabled_zero_trust_intrusion_detection_in_industrial_internet_of_things_architecture. Retrived on: 25-09-2025.
4. Harrison, A., Ullah, S., Alombah, N. H., Bajaj, M., Mbasso, W. F., Iqbal, S., & Tuka, M. B. (2024). Enhanced control strategy for photovoltaic emulator operating in continuously changing environmental conditions based on shift methodology. *Scientific Reports*, *14*(1), 13406. Enhanced control strategy for photovoltaic emulator operating in continuously changing environmental conditions based on shift methodology. *Scientific Reports*, *14*(1), p.13406. Retrieved from: https://www.nature.com/articles/s41598-024-64092-7. Retrieved on: 24-09-2025.
5. Damaraju, A., (2022). Integrating Zero Trust with Cloud Security: A Comprehensive Approach. *Journal Environmental Sciences And Technology*, *1*(1), pp.279-291. Retrieved from: https://www.researchgate.net/profile/Dash-Karan/publication/388497339_Integrating_Zero_Trust_with_Cloud_Security_A_Comprehensive_Approach/links/679b02c84c479b26c9c1df7a/Integrating-Zero-Trust-with-Cloud-Security-A-Comprehensive-Approach.pdf. Retrieved on: 25-09-2025.
6. Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), 074-086. Retrieved from: https://www.researchgate.net/profile/Olukunle-Amoo/publication/387727675_Redefining_zero_trust_architecture_in_cloud_networks_A_conceptual_shift_towards_granular_dynamic_access_control_and_policy_enforcement/links/6779937b894c55208542f523/Redefining-zero-trust-architecture-in-cloud-networks-A-conceptual-shift-towards-granular-dynamic-access-control-and-policy-enforcement.pdf. Retrieved on: 24-09-2025.
7. Parisa, S. K., Banerjee, S., & Whig, P. (2023). AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure: A Next-Generation Approach. *International Journal of Sustainable Devlopment in field of IT*, *15*, 15. Retrieved from: https://www.researchgate.net/profile/Somnath-Banerjee-13/publication/390098789_AI-Driven_Zero_Trust_Security_Models_for_Retail_Cloud_Infrastructure_A_Next-Generation_Approach/links/67fbba91d1054b0207d2f53a/AI-Driven-Zero-Trust-Security-Models-for-Retail-Cloud-Infrastructure-A-Next-Generation-Approach.pdf. Retrieved on: 25-09-2025.
8. Colomb, Y., White, P., Islam, R., & Alsadoon, A. (2022). Applying zero trust architecture and probability-based authentication to preserve security and privacy of data in the cloud. In *Emerging*

trends in cybersecurity applications (pp. 137-169). Cham: Springer International Publishing. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-031-09640-2_7. Retrieved on: 24-10-2025.

9. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. Retrieved from: https://link.springer.com/article/10.1186/s40537-024-00957-y. Retrieved on: 13-10-2025.
10. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin of Informatics*, *2*(2), 248-61. Retrieved from: https://www.researchgate.net/profile/Muhammad-Ismaeel-Khan/publication/391613291_AI-Driven_Threat_Detection_A_Brief_Overview_of_AI_Techniques_in_Cybersecurity/links/681f024cd1054b0207eda72a/AI-Driven-Threat-Detection-A-Brief-Overview-of-AI-Techniques-in-Cybersecurity.pdf. Retrieved on: 13-10-2025.
11. Yaseen, A., (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, *7*(12), pp.25-43. Retrieved from: https://www.researchgate.net/profile/Asad-Yaseen-2/publication/378594241_AI-DRIVEN_THREAT_DETECTION_AND_RESPONSE_A_PARADIGM_SHIFT_IN_CYBERSECURITY_Asad_Yaseen/links/65e12ae0c3b52a117001d426/AI-DRIVEN-THREAT-DETECTION-AND-RESPONSE-A-PARADIGM-SHIFT-IN-CYBERSECURITY-Asad-Yaseen.pdf. Retrieved on 13-10-2025.
12. Kolawole, I. (2024). Leveraging Cloud-based ai and zero trust architecture to enhance US cybersecurity and counteract foreign threats. *World J. Adv. Res. Rev*, *25*, 006-025. Retrieved from: https://www.researchgate.net/profile/Ikeoluwa-Kolawole/publication/389551725_Leveraging_Cloud-based_ai_and_zero_trust_architecture_to_enhance_U_S_cybersecurity_and_counteract_foreign_threats/links/67c73afbf5cb8f70d5c7acc2/Leveraging-Cloud-based-ai-and-zero-trust-architecture-to-enhance-U-S-cybersecurity-and-counteract-foreign-threats.pdf. Retrieved on: 24-09-2025.
13. Akbar, R., & Zafer, A. (2024). Next-Gen Information Security: AI-Driven Solutions for Real-Time Cyber Threat Detection in Cloud and Network Environments. *J. Cybersecur. Res*, *12*, 123-145. Retrieved from: https://www.researchgate.net/profile/Ali-Zafer-3/publication/385417618_Next-Gen_Information_Security_AI-Driven_Solutions_for_Real-Time_Cyber_Threat_Detection_in_Cloud_and_Network_Environments/links/6723b68277f274616d541f34/Next-Gen-Information-Security-AI-Driven-Solutions-for-Real-Time-Cyber-Threat-Detection-in-Cloud-and-Network-Environments.pdf. Retrieved on: 24-10-2025.
14. Tseng, J., Bilardi, G., Ekanadham, K., Kumar, M., Moreira, J., & Pattnaik, P. C. (2021). Encrypted data processing. *arXiv preprint arXiv:2109.09821*. Retrieved from: https://arxiv.org/pdf/2109.09821 Retrieved on: 13-10-2025.
15. De Gaspari, F., Hitaj, D., Pagnotta, G., De Carli, L., & Mancini, L. V. (2022). Evading behavioral classifiers: a comprehensive analysis on evading ransomware detection techniques. *Neural Computing and Applications*, *34*(14), 12077-12096. Reliable detection of compressed and encrypted data. *Neural Computing and Applications*, *34*(22), pp.20379-20393. Retrieved from: https://link.springer.com/content/pdf/10.1007/s00521-022-07586-7.pdf Retrieved on: 13-10-2025.
16. Munjal, K., & Bhatia, R. (2023). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, *9*(4), 3759-3786. Retrieved from: https://link.springer.com/content/pdf/10.1007/s40747-022-00756-z.pdf. Retrieved on: 13-10-2025.

17. Shukla, D.K., Dwivedi, V.K. & Trivedi, M.C., (2021). Encryption algorithm in cloud computing. *Materials Today: Proceedings*, *37*, pp.1869-1875. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2214785320355620. Retrieved on: 13-10-2025.
18. Gupta, I., Singh, A.K., Lee, C.N. and Buyya, R., 2022. Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions. *IEEe Access*, *10*, pp.71247-71277. Retrieved from: https://ieeexplore.ieee.org/abstract/document/9813692/. Retrieved on: 24-10-2025.
19. Mangayarkarasi, V. A., Vinayakan, K., & Kumar, A. D. (2024). Secure Cloud Data Storage with a Zero Trust Security Foundational Deep Learning Algorithm. *International Journal of Advanced Trends in Engineering and Technology*, *9*(2), 87-93. Retrieved from: https://www.researchgate.net/profile/Kasi-Vinayakan/publication/386458836_Secure_Cloud_Data_Storage_with_a_Zero_Trust_Security_Foundational_Deep_Learning_Algorithm/links/676a4018c1b0135465f0b0b9/Secure-Cloud-Data-Storage-with-a-Zero-Trust-Security-Foundational-Deep-Learning-Algorithm.pdf. Retrieved on: 25-09-2025.
20. Anasuri, S., (2022). Zero-Trust Architectures for Multi-Cloud Environments. *International Journal of Emerging Trends in Computer Science and Information Technology*, *3*(4), pp.64-76. Retrived from: https://www.ijetcsit.org/index.php/ijetcsit/article/view/346. Retrieved on: 25-09-2025.
21. Rao, P. M., & Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, *14*(8), 10517-10553. Retrieved from: https://link.springer.com/article/10.1007/s12652-022-03707-1. Retrieved on: 03-10-2025.
22. Aliev, I., Gazul, S., & Bobova, A. (2023, March). Virtualization technologies and platforms: Comparative overview and updated performance tests. In *AIP Conference Proceedings* (Vol. 2700, No. 1, p. 040048). AIP Publishing LLC. Retrieved from: https://pubs.aip.org/aip/acp/article-abstract/2700/1/040048/2881162. Retrieved on: 03-10-2025.
23. Ahmadi, S. (2025). Autonomous Identity-Based Threat Segmentation for Zero Trust Architecture. *Cyber Security and Applications*, 100106. Retrieved from: https://www.sciencedirect.com/science/article/pii/S2772918425000232. Retrieved on: 04-10-2025.
24. Owobu, W. O., Abieba, O. A., Gbenle, P., Onoja, J. P., Daraojimba, A. I., Adepoju, A. H., & Chibunna, U. B. (2022). Conceptual Framework for Deploying Data Loss Prevention and Cloud Access Controls in Multi-Layered Security Environments. *Int. J. Multidiscip. Res. Growth Eval*, *3*(1), 850-860. Retrieved from: https://www.researchgate.net/profile/Anfo-Pub-2/publication/391700649_Conceptual_Framework_for_Deploying_Data_Loss_Prevention_and_Cloud_Access_Controls_in_Multi-Layered_Security_Environments/links/682351068a76251f22e162da/Conceptual-Framework-for-Deploying-Data-Loss-Prevention-and-Cloud-Access-Controls-in-Multi-Layered-Security-Environments.pdf. Retrieved on: 08-12-2025.
25. Arif, T., Jo, B. and Park, J.H., 2025. A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors*, *25*(8), p.2350. Retrieved from: https://www.mdpi.com/1424-8220/25/8/2350. Retrieved on: 08-12-2025.
26. Pureti, N. (2023). Encryption 101: How to Safeguard Your Sensitive Information. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 242-270. Retrieved from: https://www.neliti.com/publications/603771/encryption-101-how-to-safeguard-your-sensitive-information. Retrieved on: 07-12-2025.

27. Papaspirou, V., Papathanasaki, M., Maglaras, L., Kantzavelou, I., Douligeris, C., Ferrag, M. A., & Janicke, H. (2022, September). Security Revisited: Honeytokens meet Google Authenticator. In *2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)* (pp. 1-8). IEEE. Retrieved from: https://ieeexplore.ieee.org/abstract/document/9932907/. Retrieved on: 02-12-2025.
28. Banala, S., & Attaluri, V. (2025). Sustainable Access Management for Cloud Instances With SSH Securing Cloud Infrastructure With PAM Solutions. In *Driving Business Success Through Eco-Friendly Strategies* (pp. 321-340). IGI Global Scientific Publishing. Retrieved from: https://www.igi-global.com/chapter/sustainable-access-management-for-cloud-instances-with-ssh-securing-cloud-infrastructure-with-pam-solutions/370056. Retrieved on: 03-12-2025.
29. Arsalan, M. S., Suryaraman, S., & Sujatha, G. (2023, January). A Rule Based Secure Network System-Prevents Log4jshell and SSH Intrusions. In *2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)* (pp. 1-4). IEEE. Retrieved on: https://ieeexplore.ieee.org/abstract/document/10083350/. Retrieved on: 08-12-2025.
30. Fahrnberger, G. (2022, June). Realtime risk monitoring of SSH brute force attacks. In *International conference on innovations for community services* (pp. 75-95). Cham: Springer International Publishing. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-031-06668-9_8. Retrieved on: 04-12-2025.
31. Abdalzaher, M. S., Fouda, M. M., Emran, A., Fadlullah, Z. M., & Ibrahem, M. I. (2023). A survey on key management and authentication approaches in smart metering systems. *Energies*, *16*(5), 2355. Retrieved from: https://www.mdpi.com/1996-1073/16/5/2355. Retrieved on: 06-12-2025.
32. Sarkar, B., Saha, A., Dutta, D., De Sarkar, G., & Karmakar, K. (2024). A survey on the advanced encryption standard (AES): a pillar of modern cryptography. *International Journal of Computer Science and Mobile Computing*, *13*(4), 68-87. Retrieved from: https://www.academia.edu/download/113977741/V13I4202418.pdf. Retrieved on: 02-12-2025.
33. Sahu, S. K. (2024). Protocol Security. In *Building Secure PHP Applications: A Comprehensive Guide to Protecting Your Web Applications from Threats* (pp. 315-346). Berkeley, CA: Apress. Retrieved from: https://link.springer.com/chapter/10.1007/979-8-8688-0932-3_6. Retrieved on: 08-12-2025.
34. Masri, R., Alouneh, S., & Shawar, B. A. (2025). A Redundant Array of Independent Disks (RAID)‐Inspired Framework for Robust Domain Name System (DNS) Security: Mitigating Distributed Denial‐of‐Service (DDoS) Attacks Through Distributed Data Encoding and Redundancy. *Security and Privacy*, *8*(6), e70085. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.70085. Retrieved on: 08-12-2025.
35. Khaskheli, G. M., Sherbaz, M., & Shaikh, U. R. (2022). A comparative usability study of single-factor and two-factor authentication. *Tropical Scientific Journal*, *1*(1), 17-27. Retrieved from: https://scientificacademic.com/index.php/tsj/article/view/3. Retrieved on: 06-12-2025.
36. Irawan, B., Sheha, K. N., Rahaman, M., Erzed, N., & Herwanto, A. (2025). Evaluating the Effectiveness of Center of Internet Security Benchmark for Hardening Linux Servers Against Cyber Attacks. *Journal of Social Research*, *4*(6), 1172-1183. Retrieved from: https://ijsr.internationaljournallabs.com/index.php/ijsr/article/view/2544. Retrieved on: 08-12-2025.