Cloud Digital Immune System: An Automated Self-Healing Framework for Cloud Security

Shivani Jagdale[1], Prafull Musale[2], Shreya Sabde[3], Dr. Jagadish S Jakati[4]
[1,2,3]*Student CSE, D Y Patil International University Pune, India*
[4]*Project Guide, D Y Patil International University Pune, India*

***Abstract*—While cloud computing offers scalability and flexi-bility, it also presents security issues such as misconfigurations, unauthorised access, and lack of ongoing monitoring. Conven-tional security approaches are often reactive and rely on manual processes. Often it leads to delayed responses and increased vulnerability.**

In this paper we propose a Cloud Digital Immune System, an automated framework that continuously monitors cloud environments, detects threats in real time and reacts immediately. The system is based on an event-driven architecture using AWS services such as CloudTrail, EventBridge and Lambda. It identifies security issues such as public S3, insecure security groups, old IAM keys, unencrypted storage, disabled logging, and unauthorised activity.It is also equipped with CloudWatch, which monitors resources at the resource level, and allows both automated and manual remediation flows.

Automated actions are triggered to reduce risks when a threat is detected, and alerts are sent by email, SNS and ChatOps

Automated actions are taken to mitigate risks on threat detection, and alerts are sent via email, SNS, and ChatOps platforms. A web dashboard gives real-time monitoring and a simple explanation of alerts is provided by an AI-based module. This system significantly reduces response time and boosts overall cloud security.

***Index Terms*—Cloud Security, AWS, Automation, Intrusion Detection, Self-Healing Systems**

I. INTRODUCTION

Cloud computing is deemed one of the most important technologies in our era as it offers flexibility, scalability, and low costs [1], [6], [11]. Today, many firms are moving their services, storage, and applications to clouds, replacing their hardware-based infrastructure with flexible and afford-able cloud-based solutions. Despite cloud computing fostering technological advancements, this technology has raised various cybersecurity threats [3], [5].

One of the primary sources of vulnerabilities related to cloud computing involves cloud configuration problems, such as misconfigured storage buckets, too broad network permis-sions, publicly available access keys, and insecure database configurations [5], [13], [15]. Unfortunately, such vulnera-bilities tend to go undetected as there is no proper way to monitor them due to lack of appropriate tools and dependence on periodic manual audits of cloud infrastructures [10].

Generally speaking, security activities performed within cloud computing infrastructure follow an alert-based approach and involve numerous human actions [6], [12]. Very often, security staff needs time to investigate the detected threat and take necessary steps to mitigate it. Moreover, threat detection and threat mitigation activities tend to be separated from each other, causing delays in security activities.

Furthermore, the absence of constant monitoring systems and real-time threat detection systems raises the chances of data leakage, service unavailability, and nonconformity with security protocols and regulations [19], [20]. This issue is mag-nified in small and medium enterprises because of inadequate resources and expertise in cybersecurity.

To mitigate this issue, the creation of an intelligent au-tomation system that can constantly monitor cloud computing systems, detect real-time threats, and execute remediation actions quickly is needed. This paper presents a Cloud Digital Immune System based on biological immune systems. The cloud digital immune system integrates continuous monitoring, automatic threat detection, intelligent remediation, and real-time notification into one integrated cloud security system with the assistance of AWS cloud platforms and AI-assisted analyses.

II. LITERATURE SURVEY

Cloud computing is popular due to its scalable, flexible, and money-saving features. At the same time, it raises multiple security-related problems. Mell and Grance [1] described the phenomenon of cloud computing, paying attention to service models' secure implementation. Sharma et al. [2] investigated various cloud security issues and concluded that data breaches, insecure application programming interfaces (APIs), and inad-equate access controls were among them.

It has been proven that security misconfiguration is one of the main reasons behind cloud computing security breaches. Hashizume et al. [5] and Modi et al. [13] indicated that improper access control, exposed storage, and weak identity management were some of the most common vulnerabilities of cloud systems. Likewise, Jensen et al. [10] noted that some of the technical threats involved data leakage and absence of adequate monitoring.

As far as traditional methods of cloud security are con-cerned, they are mainly implemented in a reactive manner. Buyya et al. [6] and Radwan et al. [12] pointed out that most of these methods involved detecting attacks once they happened, thus delaying the process and posing additional risks. The situation was made even worse by the fact that detection and remediation did not occur simultaneously.

Due to a fast-paced development of cloud technologies, event-driven and serverless architectures gained wide popu-larity. AWS Lambda provides for the automatic launch of cloud tasks triggered by events [7]. Additionally, CloudTrail and EventBridge are used for monitoring and filtering cloud activity in real time [8]. These technologies serve as a solid basis for creating automated cloud security frameworks.

Recently, researchers have considered the potential of artifi-cial intelligence in addressing cloud computing security issues. Numerous machine learning algorithms were utilized to detect anomalies, intrusions, and predict potential threats [21]. Such systems could help improve the precision of threat detection. Still, many AI-based solutions failed to implement effective integration with remediation procedures. Besides, machine learning requires vast amounts of training data.

Among the existing cloud security frameworks, OWASP
[19] and Cloud Security Alliance (CSA) [20] deserve special attention. These frameworks provided numerous guidelines for identifying and reducing cloud security threats. However, they mostly involved security practices and did not deal with automation. Commercial cloud security solutions allowed monitoring and generating alerts, yet still relied on humans for remediation.

In spite of all these developments, there is a need for an innovative approach to address the shortcomings of devel-oping a system that brings all these elements together such as continuous monitoring, threat detection, remediation, and visualization under one umbrella. The majority of the proposed approaches only cover either threat detection or monitoring; however, there is no approach that can bring an automated solution to this issue.

III. PROBLEM STATEMENT

Despite significant progress in cloud computing, providing robust security is a major issue. Previous research has shown that cloud environments are highly susceptible to security threats, such as misconfigurations, weak access controls, ex-posed storage, and poor monitoring systems. They also have the advantage of showing that these shortcomings are often the result of human error and the absence of constant automated control.

The majority of traditional cloud security solutions are reactive in nature. They can only spot threats after the fact, resulting in slower response times and a higher risk of data breaches and system compromises. Today's systems also tend to separate the detection of threats and their remediation, leading to inefficiencies in dealing with security incidents.

Although modern cloud technologies do support event-driven and serverless architectures for real-time monitoring, these features are not fully exploited in integrated security frameworks. Similarly, AI-based security solutions do make detection more accurate but do not integrate smoothly with automated response systems.

Besides, the security frameworks in the current literature are mostly guidelines, not automatic solutions, making them difficult to apply in real-

world scenarios. This problem is even more acute for small and medium sized organizations that often lack the resources and expertise to deploy complex security solutions.

This means that there's a need for a system that can monitor cloud environments in real-time, detect threats in real-time, and take immediate actions without any manual help. The aim of this research is to fill this gap by developing a Cloud Dig-ital Immune System that brings together detection, response, notification and visualization into a single framework.

IV. OBJECTIVES

- To design a continuous cloud activity monitoring system in real time.
- Identifying common security issues of cloud such as misconfiguration, public exposure of resources and unau-thorized access.
- To implement automated remediation systems that im-prove response times and reduce the need for human intervention.
- To send alerts through multiple channels to ensure people are always aware of security events.
- Develop a web-based dashboard to manage and display alerts and system status. To add an AI based module that gives simple, easy to understand explanations of security problems.
- To develop an affordable solution that can be deployed by small and medium businesses.

V. SYSTEM ARCHITECTURE

The Cloud Digital Immune System is built with a serverless, event-driven architecture. It enables real-time detection and au-tomatic remediation of cloud security threats. The system has several layers, including detection, remediation, notification, storage and visualisation.

1) Detection pipeline: The starting point for detection is AWS CloudTrail, which records all API activity that occurs in the cloud environment.Amazon CloudWatch works alongside Amazon CloudTrail to monitor resource metrics and send alerts depending on the threshold levels defined. Amazon EventBridge listens to these logs and sets up specific rules to capture security-related events such as creation of IAM keys, exposure of public resources, or configuration changes.

There are dedicated detection Lambda functions associated to each rule that fires. These functions look at the event data to determine if there is a security threat or misconfiguration. When a threat is detected, a record is created and saved in the DynamoDB alerts table.

A. Remediation flow

If a threat is detected, it immediately passes the event to the remediation layer. This layer is made up of specialized Lambda functions that are supposed to solve different security problems. The right steps are taken based on the threat found, including restricting access, turning off credentials or restoring secure settings.

Once the remediation is done, the system updates the database with the new status and logs the action for future study.

B. Notification Layer

The notification layer informs users about the identified threats and remediation actions. It uses different communica-tion channels such as SNS, email, Discord, WhatsApp. There is also a fallback SNS mechanism to guarantee delivery of alerts in the event the other channels fail.The system also supports AI based summariza- The alerts are handled to create simple human readable explanations for better understanding.

C. Storage and API Tier

DynamoDB stores alerts, responses and configuration in-formation. System configuration, alerts and remediation status are in different tables. An API layer (API Gateway and Lambda functions) is deployed. This allows the dashboard on the frontend to fetch alerts, update configurations and trigger remedial actions as necessary.

D. Dashboard and User Interaction

A web based dashboard has been developed using React to provide an easy to use interface to monitor the system. Users can view alerts, monitor remediation status, and control sys-tem settings. The dashboard communicates with the backend through REST APIs.

E. Hybrid Edge Integration

A Flask-built SOC gateway located locally connects to the cloud-hosted detection pipeline through an ngrok tunnel.The system can be integrated with local environments via a secure tunnel. In hybrid and on-premises deployments, alerts can be

received and processed by a local gateway application.

VI. METHODOLOGY

The proposed Cloud Digital Immune System in this paper adopts a structured approach with four major stages: event monitoring, threat detection, automated remediation and alert management. The system is based on an event-driven paradigm to enable real-time processing of cloud activities.

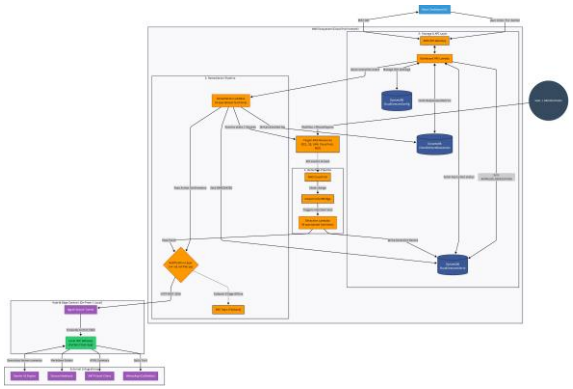

Fig. 1: System Architecture of Cloud Digital Immune System

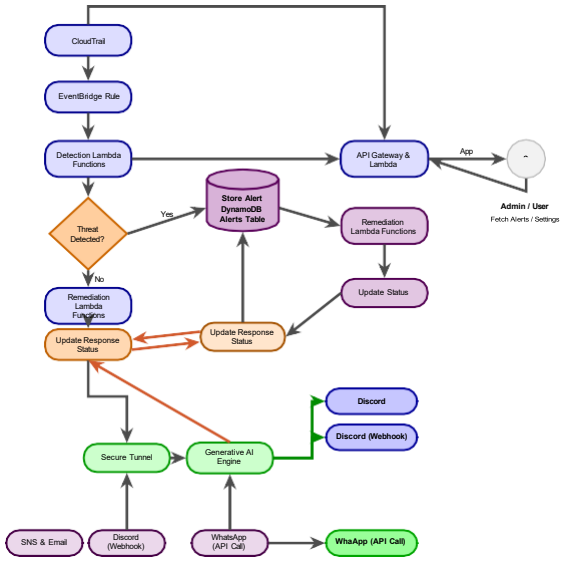

Fig. 2: System Flow of the Cloud Digital Immune System.

A. *Monitoring Events*

AWS CloudTrail logs all cloud activity continuously. This system logs API calls and configuration changes across ser-vices. These logs are the primary source of data for finding potential security issues.

B. *Threat Detection*

In Amazon EventBridge, multiple rules are configured to filter security related events from CloudTrail logs. When the matching event occurs, specific detection Lambda functions are invoked.

Each detection function is designed to detect specific types of vulnerabilities; such as

- create IAM access key
- Public access to S3 buckets
- Open ports in security groups
- Logging services disabled
- Unencrypted storage resources

Detection functions look at event data for a sign that it is a security risk. If a threat is verified, an alert record is created and stored in the database.

C. *Self-healing*

When a security issue is discovered, the system automati-cally activates remediation Lambda functions. These functions take appropriate corrective action based on the type of threat. Examples are:

- Disabling compromised IAM credentials
- Preventing access by the public to storage resources
- Enable logging configurations
- Restrict insecure network rules

If the threat level is high, then there is a process of obtaining approval by way of notifying administrators, who will have to manually approve the threat remediation activity before carrying out such an action.This automated approach reduces the response time and minimizes the dependency on manual intervention.

D. *Alert and Notification Management*

All of the discovered threats with their remediations are stored in DynamoDB. It has multiple notification channels like SNS, email and ChatOps platforms to ensure timely notification.

Further, an AI-based module generates simplified expla-nations of the alerts to help the users understand better the problem and its consequences.

E. *Visualization and User Interaction*

Web-based dashboard to display alerts, remediation status and system health APIs connect to an interactive interface where users can follow activities, review actions and manage configurations.

VII. IMPLEMENTATION

The proposed Cloud Digital Immune System is realized on AWS with a serverless architecture. It combines an extensive set of cloud services for real-time threat detection, automated remediation and centralized monitoring.

A. Detection Implementation

AWS CloudTrail is used to monitor all API activity and configuration changes happening in the cloud. We created event bridge rules to filter on specific security related events like IAM key creation, public access settings, security group changes.

If an event matches a predefined rule, it triggers detection Lambda functions. Each detection function is designed to handle a specific security problem. These functions analyze event data and determine whether it is a threat. If a threat is detected an alert record is created and stored in a dynamo DB table.

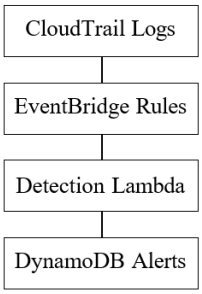

Fig. 3: Detection Pipeline Flow

B. Remediation Implementation

For each detected threat a remediation lambda function is invoked. These functions perform automatic predefined corrective actions. For example, you can disable IAM access keys, disable public access to storage, and prohibit insecure network rules.

Once the remediation action is performed, the system up-dates the response status in DynamoDB to keep track of the actions performed.

TABLE I: Detection and Remediation Mapping

Detection	Remediation Action
IAM Key Creation	Disable/Delete Key
Stale IAM Keys	Deactivate Key
Root Login	Restrict Access + Alert
Public S3	Block Public Access
Unencrypted EBS	Enforce Encryption
Open Ports	Restrict Ports
CloudTrail Disabled	Enable Logging
Unauthorized Region	Restrict Access
Public RDS	Disable Public Access

C. Notification System

For each threat detected, a corresponding remediation Lambda function is invoked. These functions do automatic predefined corrective actions. For example, you can disable IAM access keys, disable public access to storage, and disallow insecure network rules.

After the remediation action is performed, the system up-dates the response status in DynamoDB to track the performed actions.

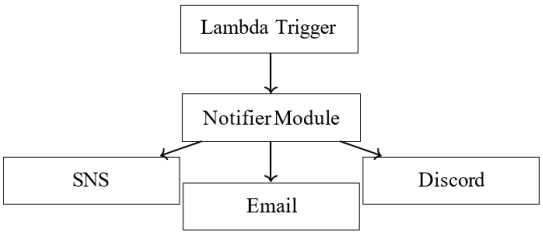

Fig. 4: Multi-Channel Notification System

D. AI Integration

The system includes an AI-based summarization module to produce human-readable explanations of detected threats. The module processes the alert data and converts the technical information into the simplified summary. It helps the user to understand the issue quickly.

In case the danger is of a high magnitude, the approval process shall involve informing the relevant administrators so that they get to manually approve the remedy for the danger prior to the execution of that activity.

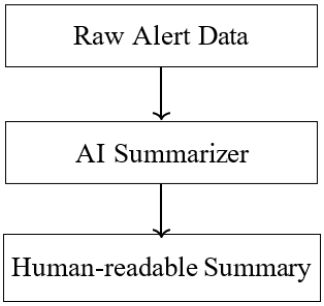

Fig. 5: AI-Based Alert Summarization

E. Data Storage

The primary data storage service is DynamoDB. The tables for alerts, remediation responses and system configuration are stored separately. This facilitates efficient querying and real-time updates.

TABLE II: DynamoDB Table Structure

Table Name	Attributes
CloudImmuneAlerts	ID, Type, Severity, Status
CloudImmuneResponses	Action, Result, Timestamp
CloudImmuneConfig	Settings, Thresholds

F. API and Dashboard

An API layer with API Gateway and Lambda functions to enable communication between the backend and the frontend dashboard. The dashboard is built using React and provides features such as viewing alerts, filtering, system monitoring, and configuration management.

The dashboard allows the user to interact with the system, view alerts, check the remediation status and trigger manual action where needed.

G. System Integration

All components are integrated with an event-driven archi-tecture to ensure seamless communication between detection, remediation, notification and visualization layers. This design enables scalability, fault-tolerance and efficient real-time processing.

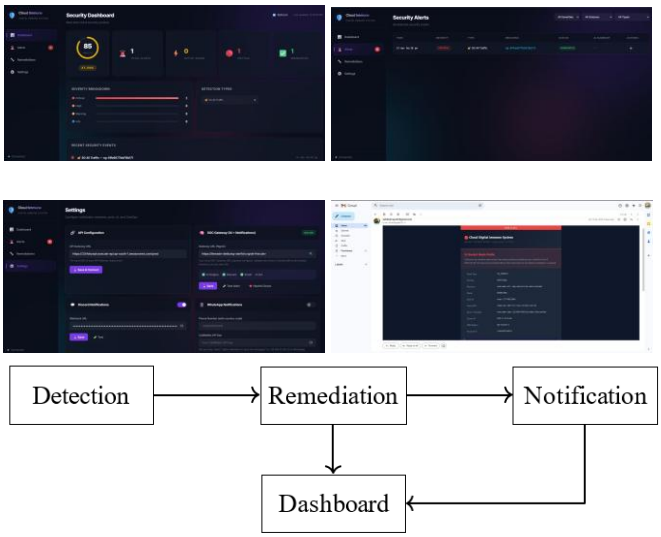

Fig. 7: Overall System Integration Flow

VIII. RESULTS AND ANALYSIS

The evaluation of the proposed Cloud Digital Immune System was done based on the detection accuracy, response time and overall efficiency of the system. We simulated multiple security scenarios, including IAM key creation, public S3 access, open ports, and disabled logging.

A. Detection Accuracy

The system managed to detect all configured security events using EventBridge rules and Lambda functions. The detection accuracy is high because of rule based filtering and real time event monitoring.

TABLE III: Detection Accuracy

Threat Type	Detection Accuracy (%)
IAM Key Creation	100
Stale IAM Keys	100
Root Account Login	100
Public S3 Access	100
Open Ports	95
Unencrypted EBS	95
CloudTrail Disabled	100
Unauthorized Region Activity	95
Public RDS	100

B. Response Time Analysis

The system was assessed on the basis of the time taken to detect and remediate threats. The automated system slashed response time dramatically compared to manual methods.

TABLE IV: Response Time Comparison

Operation	Manual (sec)	Automated (sec)
Detection	30–60	2–5
Remediation	60–120	5–10

C. Performance Comparison

It was compared to traditional methods of cloud security monitoring. The automated process yielded big gains in efficiency and reliability.

TABLE V: Performance Comparison

Metric	Manual System	Proposed System
Detection Speed	Low	High
Response Time	Slow	Fast
Human Effort	High	Low
Scalability	Limited	High
Accuracy	Medium	High

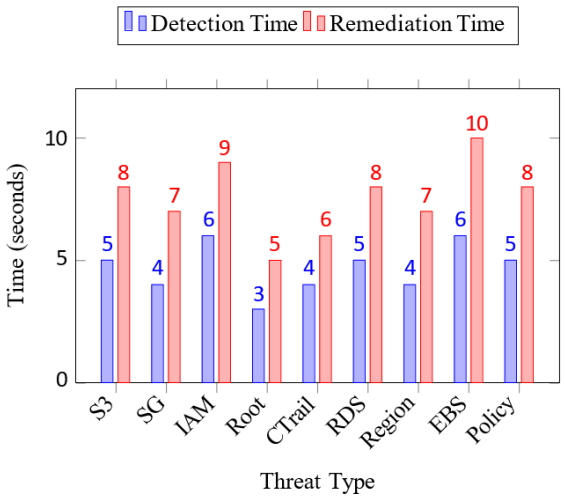

Fig. 8: Detection and remediation time comparison for differ-ent threats

Detection and Remediation Time Analysis:

This graph [Fig.8] compares the time required by the pro-posed system to detect and remediate different cloud security threats. The Cloud Digital Immune System performs rapid automated response actions after threat detection, thereby reducing the overall response time and improving cloud security efficiency.

Threat Detection Distribution:

This graph[Fig.9] represents the number of security threats detected during system testing across various cloud configu-rations and services. Public S3 exposure and insecure security group rules were among the most frequently identified threats, demonstrating the system's capability to continuously monitor and detect multiple cloud security issues in real time.

Overall System Performance Evaluation:

This graph[Fig. 10] compares the efficiency of traditional manual security management with the proposed automated framework. The proposed Cloud Digital Immune System achieved significantly higher efficiency due to continuous monitoring, instant alert generation, and automated remediation capabilities, thereby improving the overall cloud security posture.

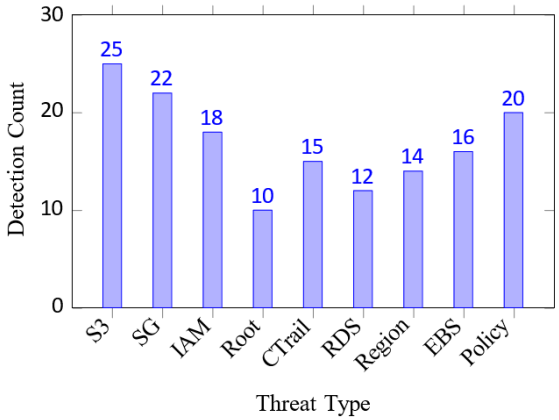

Fig. 9: Threat-wise detection frequency during testing

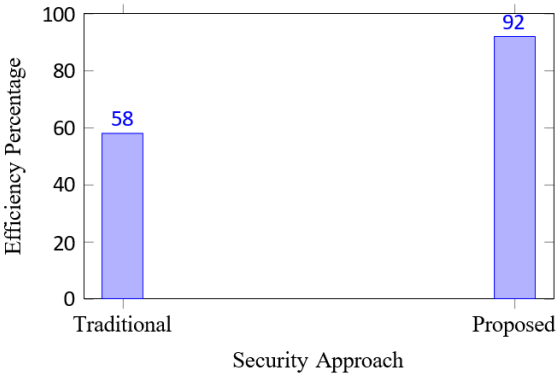

Fig. 10: Overall security efficiency comparison between traditional and proposed system

D. Discussion

The results show that the proposed system improves cloud security management significantly by reducing detection and response time. Use of serverless components ensures scala-bility and automated remediation reduces human effort. The multi-channel notification and AI-based summarisation im-prove usability and effectiveness of response.

In general, the system offers a reliable and efficient solution for real-time cloud security monitoring and automated threat handling.

IX. LIMITATIONS

The proposed system has some limitations. It is heavily tied to AWS services making it not directly

usable for multi-cloud environments. The detection mechanism is rule based which means unknown or zero-day threats may not be detected. The AI module is limited to alert summarisation only and not advanced threat prediction. Event processing might be slightly delayed and operational costs could go up for large scale deployments.

X. CONCLUSION AND FUTURE WORK

A. Conclusion

Cloud Security: A Cloud Digital Immune System is pro-posed to enhance cloud security through real-time detection and automated remediation. The system is based on AWS services such as CloudTrail, EventBridge, Lambda, and Dy-namoDB to support a scalable and event-driven architecture.It detects multiple threats such as: IAM key misuse, public access issues and resource misconfigurations. Automated re-mediation also drastically reduces the response time compared to manual methods. Multi-channel notifications and AI-based alert summaries improve usability and response efficiency. It provides reliable, scalable and efficient solution for pro-active cloud security management.

B. Future Work

- Extend support to multi-cloud environments such as Azure and Google Cloud.
- Integrate Terraform for automated infrastructure provisioning and deployment.
- Implement advanced AI techniques for anomaly detection and predictive security analysis.
- Improve hybrid cloud integration for better on-premises support.
- Enhance dashboard visualization and user interaction features.
- Optimize cost and performance for large-scale deployments.

REFERENCES

[1] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology, 2011.

[2] P. Sharma, S. K. Sood, and S. Kaur, “Security Issues in Cloud Com-puting,” in *International Conference on High Performance Architecture and Grid Computing*, Springer, 2011, pp. 36–45.

[3] M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in Cloud Computing: Opportunities and Challenges,” *Information Sciences*, vol. 305, pp. 357–383, 2015.

[4] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2013.

[5] K. Hashizume, D. G. Rosado, E. Ferna´ndez-Medina, and E. B. Fernan-dez, “An Analysis of Security Issues for Cloud Computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, p. 5, 2013.

[6] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility,” *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[7] Amazon Web Services, “AWS Lambda Documentation,” 2023. [Online]. Available: https://docs.aws.amazon.com/lambda/

[8] Amazon Web Services, “Amazon EventBridge and CloudTrail,” 2023. [Online]. Available: https://docs.aws.amazon.com/eventbridge/

[9] Google, “AI for Security Overview,” 2023. [Online]. Available: https://cloud.google.com/security/ai

[10] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, “On Technical Security Issues in Cloud Computing,” in *2009 IEEE International Conference on Cloud Computing*, 2009, pp. 109–116.

[11] M. Armbrust et al., “A View of Cloud Computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[12] T. Radwan, M. A. Azer, and N. Abdelbaki, “Cloud Computing Security: Challenges and Future Trends,” *International Journal of Computer Applications in Technology*, vol. 55, no. 2, pp. 158–172, 2017.

[13] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A Survey of Intrusion Detection Techniques in Cloud,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.

[14] A. Sajid, H. Abbas, and K. Saleem, “Cloud-assisted IoT-based SCADA Systems Security: A Review of the State of the Art and Future Challenges,” *IEEE Access*, vol. 4, pp. 1375–

1384, 2016.
[15] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843–859, 2012.
[16] HashiCorp, "Terraform Documentation," 2023. [Online]. Available: https://developer.hashicorp.com/terraform/docs
[17] Microsoft, "Azure Security Documentation," 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/
[18] Google Cloud, "Cloud Security Overview," 2023. [Online]. Available: https://cloud.google.com/security
[19] OWASP, "Top 10 Cloud Security Risks," 2022. [Online]. Available: https://owasp.org/www-project-cloud-security/
[20] Cloud Security Alliance, "Cloud Security Alliance Guidance," 2021. [Online]. Available: https://cloudsecurityalliance.org/research/guidance/
[21] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," *IEEE Access*, vol. 9, pp. 20717–20735, 2021.
[22] A. S. S. V. Agastya, B. R. Kumar, D. S. S. Varma, C. Gangu, and K. CR, "AI Based Threat Detection System," in *2025 Fourth International Con-ference on Smart Technologies, Communication and Robotics (STCR)*, IEEE, 2025.
[23] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, 2016.
[24] IBM, "Cloud Security Framework," 2022. [Online]. Available: https://www.ibm.com/cloud/security
[25] Cisco, "Cloud Security Report," 2023. [Online]. Available: https://www.cisco.com/site/us/en/products/security/