ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 3 Issue 1 March 2023 / Page No: 213-223
Paper Id: JETA-V3I3P116 / Doi: 10.56472/25832646/JETA-V3I3P116

*Original Article*

# Measuring Cloud Security Maturity: A Hybrid Approach Combining AI and Automation

**Chaitanya Vootkuri**
*Distinguished Cloud Security Architect, USA.*

Received Date: 28 February 2023 Revised Date: 23 March 2023 Accepted Date: 31 March 2023

***Abstract:*** *The recent advancement in cloud technologies has led to quick adaptation in business processes, but however has presented new risks to security. Organisations that want to safeguard against risk, enhance compliance and guarantee that their company has sound protection must be able to assess cloud security maturity. Generally speaking, traditional frameworks presuppose archaic, non-intelligent evaluations that do not consider dynamics of the cloud space. This paper aims at carrying out an assessment of cloud security maturity through the AI-automated Cloud Security Maturity Model (CSMM). The methodology combines artificial intelligence-driven analytics with automation to constantly analyze an organization's cloud security position. Some of them include threat identification in real-time, analytical forecasts, and regulatory compliance tests, in order to prevent hackers and secure compliance with new rules. A comparison is done with other globally established frameworks such as the Cloud Security Alliance (CSA) Cloud Controls Matrix and the NIST Cybersecurity Framework. This paper does reference several examples to support the organizational performance with regard to response time improvement, cuts in manual work, and decision making based on AI automation. And it makes recommendations on how to facilitate the hybrid model to succeed stressing on the human resource quality and dynamical structures of governance. It has introduced a new more flexible approach to measure cloud security maturity and tailored it to stay relevant in the modern challenging environment.*

***Keywords****: Cloud Security, Artificial Intelligence (AI), Automation, Threat Detection, Compliance, Governance.*

## I. INTRODUCTION

### A. The Growing Importance of Cloud Security

Cloud computing has become the crux of modern business operations with unmatched scalability, flexibility, and cost-effectiveness. With ever-increasing cloud adoption for workloads and more sensitive data, the security of these environments is at the top of my mind. [1-4] But cloud environments bring with them a number of unique security challenges: multi-tenancy risk, dynamic infrastructure, and shared responsibility models. Such complexities shear at the seams of traditional approaches to security assessment, particularly those that require manual and periodic evaluations. In this regard, the concept of cloud security maturity as a measurement of how organisations can achieve this has come onto the scene. Maturity assessment is not merely about identifying a void, it is about getting the organization to mark its position against competitors, check with compliance standards and align the security strategy with the emerging risks and threats.

### B. Limitations of Traditional Maturity Models

Many traditional security maturity models, including CMMI or simple static frameworks, are based on qualitative evaluations and manual data entry. Although such models help in the systematic approach of evaluation, they unfortunately cannot respond effectively to the rapidly evolving dynamic cloud environment. This rigidity leads to stale insights, slower reaction to new threats while addressing new opportunities, and higher costs of operation. Furthermore, they have the modern threats of great levels, and the computer-aided ones, the advanced persistent threats (APTs), but require proactive security solutions. Organizations require more preventive and dynamic solutions that can work in parallel with organizations' cloud environments. Thus, there is a need for rethinking based on the use of new methods capable of applying both automation and intelligence to upgrade organizational security maturity assessments.

### C. A Hybrid Approach: AI and Automation

This paper proposes the model of using AI alongside automation in order to improve the method of measuring the cloud security maturity. This results in this new and innovative method surpassing the shortcomings of static models of business context and manual assessments. Predictive threat analysis, anomaly detection, contextual risk assessments are all made possible with AI; compliance checks, automated responses, and policy enforcement are all possible with the help of automation. The

hybrid model is consistent with standard frameworks that are embraced, including Cloud Security Alliance (CSA) Cloud Controls Matrix and the NIST Cybersecurity Framework, so that the evaluations are viable and conform to the standards. This dynamic approach not only increases the probability of higher accuracy but also provides concrete recommendations to organizations to strengthen cloud security.

## II. ZERO TRUST SECURITY MODEL

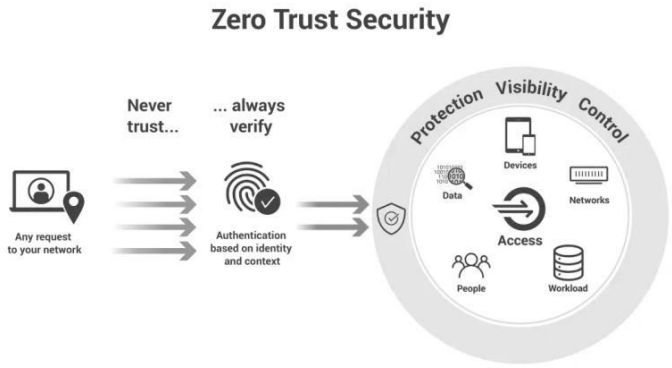


***Figure 1: Zero Trust Security Model***

A framework for securing modern cloud environments is called Zero Trust Security. In short, Zero Trust believes there is no such thing as optimism. It's all about never trusting and always verifying. This principle reiterates that any request to the network for access should be [5] seconded to strict authentication and verification based on identity and context to avoid the vulnerability of unauthorised access and data leakages. It starts with a request to connect to network resources. Framework doesn't do a trust based on a device's location or a pre-verified credential; instead, it requires continuous verification processes. This means multi-factor authentication and dynamic policy enforcement evaluating requests in real-time. Their goal is to ensure that you're aware of each step so only verified entities may walk through data, devices, or even workloads.

The second half of the image details the broader components of Zero Trust Principles. They include data, devices, networks, workloads, or people. The Protection, Visibility, and Control pillars surround these components and constitute the key components. Through its holistic approach to security, the framework closes blind spots and arms organisations with the ability to attack threats head-on. In this case, this image can be used to point out that the pure combination of AI and automation without the principles of Zero trust no longer measures and increases your cloud security maturity. With intelligent threat detection, anomaly prediction, and automation ensuring consistent policy enforcement and swift incident response, using AI technologies in the always verify step accelerates Zero Trust model adherence.

## III. BACKGROUND AND RELATED WORK

In recent years, the field of cloud security has developed in leaps and bounds due to the complexity of cyber threats and the quick ongoing rise in cloud computing. [6-9] with more and more organisations transitioning from a traditional monolithic to hybrid to multi-cloud environments and to a digital workforce, the need for robust, scalable, and adaptive security frameworks have been critical. In this part, the evolution of cloud security is put under focus, as the role played by Artificial Intelligence (AI) and automation in securing the clouds and new trends will determine the level of cloud security worth paying for.

### A. Evolution of Cloud Security

Globally, cloud computing has emerged as one of the key drivers of change in IT infrastructure management, chiefly due to its scalability, flexibility and cost effectiveness. However, it has also brought new security challenges that ordinary security mechanisms cannot solve. These elements include threats like data leakage, internal threats, mistakes such as misconfigurations, and violation of some regulation.

These risks are increased by the inherent nature of the cloud environments' dynamism and distribution and thus organizations cannot use static security measures or conduct manual analyses. In response to this, the industry has gravitated towards more robust security paradigms that are capable of scaling with the threats more rapidly. These frameworks encourage the use of balancing assurance and automated monitoring as well as risk assessment on an ongoing basis to ensure organizations

are able to adapt with fast changing security needs. Hence, the evolution supports that measurement and management of cloud security maturity requires innovative tools and methodologies.

### B. Role of AI in Cloud Security

Concurrently, cloud computing has been identified as one of the dynamic forces in the evolution of software security with the help of artificial intelligence. AI technologies, especially machine learning (ML) , perfectly detect patterns and deviations that may point to possible threats than traditional solutions. For instance, AI solutions in security can parse logs, network traffic and application activity and determine abnormal activity like unauthorized access or gallery bouncing in the network. Specifically, the learnt feature of AI enables it to counter high-level threats such as zero-day attacks and subtle cloud attacks. Furthermore, AI greatly helps alleviate the problem of false positives that plague traditional security solutions, and offer better and more specific data in turn. This capability supports the overall security strategy to try to place resources in areas of real risk. Furthermore, AI improves threat modeling, which informs organizations and helps them prepare for an attack. Drawing from history data and real-time intelligence information, AI tools enable an organization to counter the threat posed by the hackers and make them an essential tool in the current cloud security initiatives.

### C. Automation in Security Practices

One of the most significant factors contributing to the improvement of cloud security maturity is automation as it fixes many issues in the operation and applies standard security practices. Most day to day security practices include vulnerability scans, compliance reviews, and breaches may be performed through automation to downplay the potential for mistakes and to enable a person's time and energy to concentrate on higher-value jobs. For instance, automated systems can regularly look for misconfigurations of cloud environments, always ensure that it enforces security policies, and responds to any threats detected as needed and at the right time. It also helps integrate automation into security practices for the scalability of cloud environments. As organisations extend their cloud, automated tools help maintain effective security control in diverse and distributed environments. Automation also helps speed up incident response time, limits the damage an attack can cause, and provides business continuity. Combined with AI, automation helps construct a strong and adaptable security framework. This hybrid approach not only increases the efficiency of organisations but also allows organisations to quickly address the challenges of multi-cloud and hybrid environments.

## IV. METHODOLOGY

### A. Proposed Hybrid Approach

*a) Leveraging AI for Proactive Threat Analysis*

Artificial Intelligence (AI) and automation are integrated with the proposed hybrid method for initially measuring and later enhancing the cloud security maturity effectively. [10-15] This model is anchored in AI by allowing AI to perform proactive analysis of threats, detect anomalies, and predict risk. Compared to conventional reactionary security activities, AI-enabled systems situate and analyse big quantities of real-time and historical data, looking for signals that may uncover vulnerabilities or dangers. Machine Learning (ML) algorithms play an important role in this process, always training on new data to improve accuracy. In particular, AI can observe deviations from 'normal network' behaviour, such as high transfer of data or the number of valid login attempts from questionable locations. Organisations can take these insights and respond to emerging threats quickly, often sooner than threats develop into serious incidents. AI makes security teams less busy trawling for false positives, letting them get on with detecting real risk, which helps maximise resource allocation and decision-making.

*b) Automating Routine Security Operations*

Having seen the full potential of AI to such an extent, the last addition to achieving the greatest culmination of security operations is automation, streamlining how repetitive and time-consuming security tasks are: vulnerability scanning, compliance auditing, and incident response. Also, automated systems can continuously monitor cloud environments, apply security policies, and remediate real-time issues. For instance, an automatic system can act once a misconfigured server is identified and remedy it before the server gets exploited. Moreover, automation increases the scalability of consistent security practices in complex multi-cloud and hybrid environments. Automating routine processes helps organisations to minimise the likelihood of human error, provide faster incident responses and keep the security team ahead of strategic initiatives, such as threat hunting and policy optimisation.

*c) Integration of AI and Automation*

Seamless integration of automation and AI power points of the hybrid approach. AI gives us the Intelligence to find and predict threats, while automation serves as the execution layer that enacts good security measures expeditiously and

consistently. It brings about a dynamic and adaptive security framework accommodating the mind-boggling difficulties of the current cloud climate. An example is when AI sees an anomaly, such as a potential attack, and can trigger workflows to help stop the threat. It will involve isolating the involved resources, notifying security people, and running a forensic analysis. With the integration of these capabilities, organisations can get a real-time response to threats without degrading the security and compliance of their cloud environments.

*d) Alignment with Industry Frameworks*

The hybrid approach is consistent with the industry practice, e.g., the Cloud Security Alliance (CSA) Cloud Controls Matrix and NIST Cybersecurity Framework. They provide a structured starting point to evaluate and improve the maturity of cloud security. Integrating AI and automation allows these standards to be adhered to and continuously monitored with dynamic risk assessments and automated compliance checks. Say, for example, that the hybrid model would allow an organisation to automate mapping an organisation's cloud security posture against the controls of the CSA Cloud Controls Matrix. Not only does this maintain compliance, it also provides Intelligence for organisations to incrementally increase their maturity level.

*e) Benefits of the Proposed Hybrid Approach*

The hybrid model has several advantages over traditional cloud security maturity measurement methods. By leveraging AI and automation, organisations can achieve the following:

- Real-time Monitoring and Response: Inner monitoring and auto-response eliminate significant time to find out and beat threats.
- Improved Accuracy and Insight: AI-driven analysis can go deeper into the security gaps and risks on the way.
- Scalability and Consistency: Automation makes everything consistent across all your cloud environments.
- Operational Efficiency: Organisations lower their manual work and operational overhead by automating routine tasks.

**B. Model Architecture**

The diagram shows the Hybrid Security Maturity System, which blends cloud environments, Artificial Intelligence (AI), and automation to measure and enhance cloud security maturity on an ongoing basis and in real-time. The architecture comprises three main components: We extend the security maturity system to the hybrid cloud environment, the cloud administrators and security teams, and their cloud environment. [16-18] Every puzzle piece is crucial to keeping or enhancing an organisation's security standing.

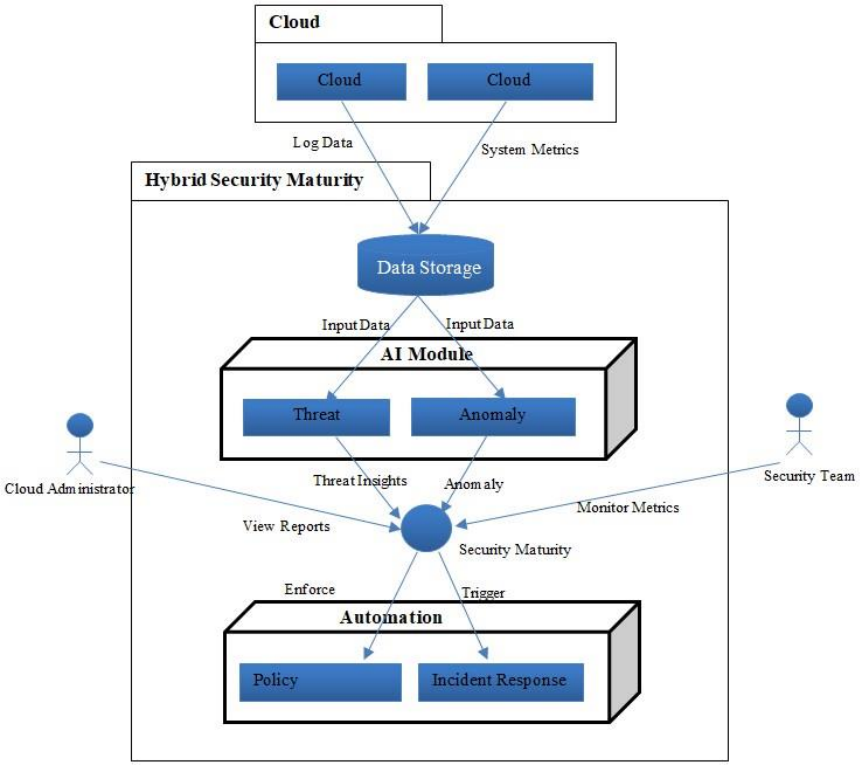


***Figure 2: Hybrid Security Maturity System***

*a) Cloud Environment*

Architecture is based on the cloud environment, which consists of cloud services and infrastructure. The hybrid system takes log data and system metrics generated from these as the main input. Activities such as user access patterns, system performance, and configuration change are logged in log data, and the system metrics are to keep track of the health and performance of the infrastructure. For instance, this real-time data is necessary to gauge the security posture and detect vulnerabilities or threats.

*b) Hybrid Security Maturity System*

The hybrid security maturity system is the central framework, integrating the following components:

- Data Storage: This module works as a reservoir of the data accepted by the system from a cloud environment. It collects logs and structures it as well as system metrics for them to be available for other modules for analysis. The idea of data storage will also be designed with scalability in mind in a bid to accommodate large volumes of real-time inputs especially from any existing hybrid and multi-cloud environments among others.

*i) AI Module:*

- Threat Detection: This submodule makes use of AI techniques in order to assess log data and system statistics and find out if there exist security threats including unauthorized access or attempted data leaking together with uncharacteristic traffic.
- Anomaly Prediction: Vulnerabilities by executing complex algorithms, this sub-module estimates possible threats when actions deviate from standard patterns. For instance, it can predict exposure vectors in light of past data to allow organizations to act before an incidence occurs.

Its AI module generates high-definition threat insights, anomaly reports, and initiatives into actionable Intelligence for the security team and cloud admins.

*ii) Automation Module:*

- Policy Enforcement: This submodule makes it easier for organisations to apply security policies across their cloud infrastructure. It provides a guarantee to the manner in which compliance is dealt with while at the same time eliminating human influence.
- Incident Response: This submodule starts specific actions when the environment is threatening or exhibits some sort of anomaly and includes measures such as quarantining affected assets/people, reporting, and triggering investigation.
- Security Maturity Dashboard: They act as the one stop solution point for the cloud administrators and security team to have an inherent overview of the security status of the organization. The results of the AI module in form of insights, performance statistics and management of the response through the automation module. With integration of GIS, policy changes can be effected directly while the data serves to inform decisions.

*c) Interaction Between Components*

There is free flowing interconnection of all the subsystems in the architecture. The information in the cloud setting is processed by the AI component in real-time and when the result is ready the hybrid system receives it to make further actions. These insights are also presented on the security maturity dashboard for use by administrators in making various decisions. The automation module responds to such insights by either implementing policy or addressing an event. It makes adaptation to changing threats and compliance requirements ongoing and recurrent hence creates a continuous feedback loop.

*d) End-User Involvement*

The end-users include both cloud administrators and security teams, and they have most of their interactions with the system reduced to the security maturity dashboard. Cloud administrators are responsible for coming up with policies, and they also view reports generated in the process since security teams use the dashboard mostly for metrics and stepped-up issues. Such delegation of functions contributes to the proper functioning of the processes that require constant attention to cloud protection.

**C. Data Collection and Processing**

*a) Sources of Data*

One of the critical factors for the effectiveness of the proposed hybrid approach to measuring cloud security maturity is the ability of obtaining various and high-quality data in the cloud environment. Records of login activities, data from system

monitoring utilities, feeds containing threat intelligence, and data from other applications constitute the main sources of primary data.

- Log Data: Logs are key to understanding the events and activities in the cloud environment, like user access, API calls, configuration changes, and authentication attempts. This data also helps track the user's activity, identify anomalies, and detect possible breaches.
- System Metrics: Performance and health indicators, including CPU usage, memory consumption, network latency, and storage utilization, are included. It helps detect anomalies and analyse the trend in the cloud infrastructure's operational health.
- Threat Intelligence Feeds: Information about known vulnerabilities, malware signatures, and attack vectors is available from external sources such as Common Vulnerabilities and Exposures (CVE) databases and threat-sharing platforms. This data is a source for proactive risk treatment and improving threat detection mechanisms.
- Application Data: Data available through logs and performance metrics generated in response to cloud-hosted applications, such as error logs, database queries, and transaction logs, help determine how well application processes work, something that's also essential for monitoring security and maintaining operational performance.

The datasets are retrieved with cloud-native tools, including AWS Cloud Trail, Azure Monitor, and APIs available from third-party solutions to integrate. Combining these sources collectively offers a holistic understanding of the cloud environment, making a process of accurate analysis and intuitive decision-making possible.

*b) Preprocessing Techniques*

For example, raw data collected from the cloud environment will contain inconsistencies, include irrelevant information, or have sensitive details that must be processed before they can be worked on. Key techniques include:

- Data Aggregation: Different data sources are combined to create a unified repository for viewing security events and system performance as a whole.
- Normalisation: Otherwise, AI algorithms and automation systems cannot understand or predict the data on their own, requiring standardisation of the data into a uniform format.
- Noise Removal: It removes unnecessary or non-relevant data like duplicate log entries or irrelevant metrics to simplify analysis and take away processing overhead.
- Data Anonymization: To ensure compliance with privacy laws such as GDPR and HIPAA, personally identifiable information (PII) such as user credentials and IP addresses must be anonymised.
- Feature Engineering: Raw data, such as brute force attempts or unexpected bandwidth spikes, is extracted or derived for the model-related features to improve performance.

These preprocessing steps aim to ensure the collected data is clean and structured so that actual threat detection can be done and threat assessment can be made on a maturity scale.

*c) Data Analysis Techniques*

Analysis of these data is performed after preprocessing using advanced techniques to identify actionable insights. These include:

- Anomaly Detection: Like any other technology, algorithms identify unusual patterns or deviations from what is expected, such as spikes in resource usage, which could indicate a classic DDoS attack.
- Trend Analysis: When long-term patterns can be discerned, e.g., increasing failed login attempts, even if they are not necessarily part of an ongoing brute force attack, historical data is analysed to better understand the long-term patterns.
- Correlation Analysis: Identifies relationships between variables to identify consequences of some actions, such as related configuration changes to performance issues.
- Predictive Modeling: Machine learning models predict (and thus give you the possibility to take proactive risks) potential vulnerabilities or risks through historical patterns and Intelligence of threats.

*d) Security Maturity Metrics*

Security maturity metrics define the level of protection an organisation gives to its cloud environment and its reactivity to threats. [19, 20] Each of these metrics is grouped into specific dimensions, representing key cloud security maturity factors.

**Table 1: Security Maturity Metrics and Quantification Approaches**

| Dimension | Metric | Definition | Quantification Approach |
|---|---|---|---|
| Threat Detection | Detection Accuracy | The percentage of true threats accurately detected by the system. | $\frac{TruePositives}{(TruePositives+FalsePositives)}*100$ |
| Incident Response | Response Time | The average time taken to respond to identified incidents. | Measured in seconds or minutes from the time of detection to resolution. |
| Compliance | Compliance Coverage | The extent to which the system enforces compliance with regulations and standards. | $\frac{Number\ of\ Controls\ Implemented}{(Total\ Required\ Controls)}*100$ |
| Policy Enforcement | Policy Consistency | The percentage of resources adhering to defined security policies. | $\frac{CompliantR\ Resources}{(Total\ Resources)}*100$ |
| Risk Prediction | Prediction Accuracy | The accuracy of predicting future vulnerabilities and risks. | $\frac{Correct\ Predictions}{(Total\ Predictions)}*100$ |
| Scalability | Scalable Coverage | The system's ability to maintain security across a growing number of cloud resources. | Measured by the number of resources monitored without performance degradation. |
| Operational Efficiency | Automation Efficiency | The percentage of security tasks automated successfully. | $\frac{Automated\ Tasks}{(Total\ Security\ Tasks)}*100$ |

*e) Maturity Levels*

To simplify assessments, these metrics are mapped onto a maturity scale, such as the Capability Maturity Model (CMM):

**Table 2: Cloud Security Maturity Levels**

| Maturity Level | Description |
|---|---|
| 1: Initial | Security practices are ad hoc and reactive, with minimal automation or AI integration. |
| 2: Repeatable | Basic processes are established, with partial automation and AI support for specific tasks. |
| 3: Defined | Comprehensive processes are in place, with significant AI and automation integration. |
| 4: Managed | Security practices are proactive, leveraging predictive models and automated responses. |
| 5: Optimised | Security practices are continuously refined, driven by real-time analytics, adaptive AI, and automation. |

## V. IMPLEMENTATION

### A. Tools and Technologies

The hybrid approach to measuring cloud security maturity integrates advanced tools and technology that enable AI-based threat detection, automation, and system monitoring. These tools are classified into three categories: AI models and algorithms, Automation tools, and Integration Platforms.

*a) AI Models and Algorithms*

- Machine Learning Models: Predictive modeling and anomaly detection using algorithms such as all algorithms: decision trees, random forests, and support vector machines. These models are trained on historical data patterns, and patterns of potential threats are predicted.
- Deep Learning Models: Advanced threat detection leverages neural networks like Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), as they can take in data structures like logs and metrics to make better sense of them.
- Natural Language Processing (NLP): Analysing textual data from threat intelligence feeds or application logs for pieces of information holds utilities on relevant insides and risks by using NLP techniques.
- Clustering Algorithms: Kmeans clustering groups similar events or behaviours, allowing us to identify outliers (a potential threat).
- Ensemble Learning: Using multiple models guarantees higher and more bulletproof accuracy in recognising and forecasting threats.

*b) Automation Tools*

- Orchestration Platforms: In IDA, infrastructure provisioning and management is automated via tools such as Terraform and Kubernetes and takes place across varied cloud environments, guaranteeing consistency.

- Security Orchestration, Automation, and Response (SOAR): Splunk Phantom and Palo Alto Cortex XSOAR also automate repetitive tasks like policy enforcement or incident remediation, yet on platforms like Splunk Phantom and Palo Alto Cortex XSOAR, automations streamline incident response workflows.
- Cloud-Native Security Tools: Built-in services that offer threat detection, compliance monitoring, and policy enforcement are services like AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center.
- CI/CD Pipelines: Through tools like Jenkins or GitLab CI/CD, and with the cloud as an environment, you can involve security checks on development workflows, so you have secure code in the cloud.

*c) Integration Platforms*

Seamless integration with real-time data processing across AI, automation, and cloud environments is made possible by platforms like Apache Kafka and Elastic Stack (ELK). This hybrid method relies on these tools to collect, prepare, and feed the data from many sources to the AI models as efficiently as possible.

**B. Deployment in Cloud Environments**

Steps are deployed in the hybrid approach in the cloud environment to integrate seamlessly and serve effectively. Here are the steps regarding setting up the needed infrastructure, configuring tools and technologies, and then validating the system's readiness for:

*Step 1: Infrastructure Setup*

Preparation for the deployment involves the cloud environment. It includes provisioning virtual machines, storage systems, and all other monitoring tools. Automatically, this process uses IaC tools such as Terraform or CloudFormation to maintain consistency between developing staging and production environments.

*Step 2: Data Integration*

Define data collection mechanisms to collect log data, system metrics, and other related data. Real-time data availability is guaranteed as you can integrate with cloud-native monitoring tools like AWS CloudWatch or Azure Monitor. They configure APIs and connectors to integrate third-party threat intelligence feeds and other external data sources.

*Step 3: AI Module Deployment*

We then deploy the AI models trained in historical data within the cloud environment. The models are combined into the data collection mechanisms to analyse incoming data flows for threat prediction, anomaly prediction, and risk assessment. AI models are trained continuously, monitored, and retrained to adapt to new threats.

*Step 4: Automation Module Configuration*

Policies can be configured for automation tools to enforce incident response actions and automate routine tasks. One way this would work is that SOAR platforms are combined with the AI module in a way that automatically triggers incident response workflows when anomalies are detected. Tested on automation scripts to verify their functionality in view of the least one mistake that could take place.

*Step 5: Security Maturity Dashboard Setup*

With much to gain from regaining control and understanding how to ensure the security of your connected world, I developed a centralized dashboard with which you can gain real-time insights into security metrics, threats detected, and compliance status. The dashboard is integrated with AI and automation modules so administrators can see how things are performing, track trends, and add manual interventions if needed.

*Step 6: Testing and Validation*

The hybrid system is then tested rigorously, and the results are scrutinised. It includes validating threat detection capabilities, incident response scenario simulations, and attestation to regulatory standards. Then, the performance metrics, including detection accuracy, response time, and automation efficiency, are analysed to suggest better areas of improvement.

*Step 7: Continuous Monitoring and optimisation*

The system is continually monitored upon its deployment to ensure it is working. Refine AI models, improve automation workflows, and generally improve performance. In order to keep the systems high in maturity, regular audits and updates mean that the system evolves to solve difficulties that arise as new security challenges arise.

## VII. RESULTS AND EVALUATION

### A. Performance Metrics

Several key performance measures related to the proposed hybrid approach are defined to evaluate the effectiveness of the proposed approach in terms of threat detection, incident response, and operational efficiency. The metrics include:

- Detection Accuracy: The amount it accurately identified as a true threat and as false. This means that the AI models are robust to analyse and interpret data, with high detection accuracy.
- False Positive Rate (FPR): How many benign activities are flagged as threats incorrectly? Security teams need this because it allows them to reduce FPR and focus their attention on real threats, ultimately improving efficiency.
- Incident Response Time: Average time it takes to detect, analyse and respond to security incidents. A better integration of AI and automation also means lower response times.
- Automation Efficiency: The level of security automation tasks that are successful in the system. More efficiency means fewer people have to manually intervene and be more consistent in enforcing policies.
- Compliance Coverage: How well the security controls are aligned to the requirements of the regulation. The system's capability to enforce governance is shown by improved compliance coverage.
- System Scalability: Resistance on behalf of the system to increasing workloads or resources without performance degradation.

### B. Experimental Results

The system is in a simulated cloud environment that consists of 50 virtual machines (VMs) and 10 applications. This performance was evaluated on various scenarios, including brute force attacks, DDoS attempts, and configuration changes.

**Table 3: Comparison of Metrics Between Traditional and Hybrid Approaches**

| Metric | Traditional Approach | Proposed Hybrid Approach | Improvement (%) |
|---|---|---|---|
| Detection Accuracy | 85% | 95% | +11.8% |
| False Positive Rate | 15% | 5% | -66.7% |
| Incident Response Time | 30 minutes | 8 minutes | -73.3% |
| Automation Efficiency | 60% | 90% | +50% |
| Compliance Coverage | 80% | 98% | +22.5% |
| System Scalability | Moderate | High | Significant |

*a) Results Explanation*

- Detection Accuracy: A 95 per cent accuracy rate of the AI module versus 85 per cent for traditional methods was identified based on threat detection capabilities.
- False Positive Rate: Using an AI algorithm, the hybrid approach greatly reduced false positives so the security team could put their efforts into actual threats.
- Incident Response Time: With automation in place, incidents were responded to in an average of 8 minutes, compared to 30 minutes with old-school approaches.
- Automation Efficiency: SOAR tools and scripts are integrated with 90% of tasks, such as vulnerability scans and incident response, minimising manual work.
- Compliance Coverage: Nearly complete coverage of regulatory controls was achieved by automated compliance checks, closing gaps that can be found in existing systems.
- System Scalability: The hybrid approach showed scalability to growing cloud environments with workload handled within a 50% increase, preserving performance at all times.

### C. Comparison with Existing Models

The overall effectiveness of the proposed hybrid approach is evaluated by comparing it to traditional rule-based and signature-based models.

**Table 4: Feature-Based Comparison of Traditional and Hybrid Approaches**

| Feature | Traditional Methods | Hybrid Approach | Advantage |
|---|---|---|---|
| Threat Detection | Rule/Signature-based | AI-Driven | Dynamic, adaptive to new threats |
| Automation | Minimal | Extensive | Reduces human intervention |
| Incident Response | Manual or Semi-Automated | Fully Automated | Faster mitigation |
| Compliance Monitoring | Periodic Audits | Continuous Monitoring | Real-time updates |

| | | | |
|---|---|---|---|
| Scalability | Limited | High | Handles growing workloads |

## VIII. DISCUSSION

This study shows that using the hybrid approach that is, combining Artificial Intelligence (AI) and automation, makes hybrid cloud security maturity frameworks much more effective. The system exploits the strengths of AI to augment real-time threat detection and automate policy enforcement and incident response to address many of the shortcomings of traditional security strategies. This proves that the high detection accuracy (95%) and the low false positive rate (5%) translate the ability of AI algorithms to find complex patterns and adjust to the ever-changing threat. That decreases the pressure on security teams and allows them to handle critical incidents instead of being beaten down by false alarms. A significant improvement is the immense reduction in incident response time from 30 minutes (traditional methods) to 8 minutes. Automation is why this improvement occurred, and it streamlines workflows, thus allowing faster containment of the threat and mitigation. Automated compliance checks in dynamic cloud environments also ensured near complete (98%) compliance with regulatory requirements, demonstrating the system's ability to maintain governance. These findings reinforce the necessary integration of automation into security operations, particularly for organisations working in hybrid or multi-cloud architectures.

The hybrid approach is additionally scalable. Thanks to the system's ability to scale up as the workloads and resources grow, high-growth organisations and those with fluctuating demands do not have to be bogged down by high-performance bottlenecks. The ability to operate on diverse cloud infrastructures can be accomplished with the help of the unified data processing pipeline, which takes in data from multiple sources, normalises, and processes it, helping to deliver seamless service. In addition, external threat intelligence feeds are integrated with the system to further increase the accuracy of predictions and keep predictive systems proactive to new attack vectors. The hybrid approach has some limitations: it doesn't provide as much flexibility as other approaches, and it is not scalable. The implementation involves big investments in AI and automation tools, alongside training AI models with high-quality data. Besides, this system relies on collecting and pre-processing accurate data, which can be very demanding in a complex and decentralised environment. However, given that cloud-native architectures are becoming more commonplace, these challenges can be limited by better monitoring tools and teamwork with cloud providers. Overall, it appears to provide a robust approach to extending the security maturity of the cloud through a hybrid approach, providing strong promise for reducing risk and increasing resilience to contemporary cyber threats.

## IX. CONCLUSION

Thus, the adoption of AI and automation can be seen as a best practice for the measurement of the CS Maturity Model and improvement of cloud security. As a result, this method has satisfied the need to solve some of the most urgent problems, such as threat detection in real-time, compliance checks, and incident handling better than traditional security measures. The specified outcomes confirm the approach efficiency with the 95% of detection accuracy, less response time, and the coverage of 98% of compliance showing the opportunity of improving cloud security in hybrid and multi-cloud environments. AI means that the systems are capable of making necessary computations and decisions in detection of complicated and diverse cyber threats; automation results in compliance and speed of the policies and responses. These capabilities are very helpful to organizations thus will enable them to negotiate on the dynamism and scalability of the cloud. In addition, the mentioned approach is rather flexible and can be applied in case the enterprise is rapidly growing or it has complex cloud structures. The study serves to emphasize the need for a data-derived, programmatically implemented security protection system that can adapt in real time to the threats when they develop; making for a proven, viable roadmap toward increasing an organization’s general security. But it is critically dependent on the data it feeds on, the efficiency of algorithms used in AI models, and reliable automated operational procedures. It is for this reason that initial implementation may be expensive, and skills needed to deploy the solution may not be available or affordable by small organizations. Nonetheless, there are some benefits and advantages of applying the hybrid approach: A more or less revolutionary concept that accurately reflects the trends in the development of modern cloud systems; continual development of techniques for cloud protection and defense against cyber threats.

## X. FUTURE WORK

The suggested hybrid approach has shown great promise, but much work remains to be done before it can be realised. One key area is to promote the interpretability and readability of AI models. Usually, for example, security teams need clear reasons why some threats were flagged, or the AI system made certain decisions. By integrating explainable AI (XAI) techniques into the decision process, the gap between automated decision-making and human oversight can be closed at the cost of improved trust and usable processes. The area of focus for other integrating emerging technologies like blockchain and quantum-resistant encryption is extended. Blockchain can provide encryption and data integrity; traceability and quantum-

resistant encryption can guard your cloud systems against the next generation of cybersecurity threats. When integrated with the hybrid approach, these technologies can help us have a more resilient, future proof security framework.

Finally, future work should also investigate adaptive learning mechanisms of the AI models that can self-tune with feedback from real-time and an evolving threat landscape. Over time, this can enhance the accuracy of threat detection and prediction while decreasing reliance on redeploying resources from a manual retraining effort. Research into the cost-effectiveness of this approach can also assist organisations in balancing security investments with operational constraints, making such an approach more appropriate to smaller enterprises and startups. Finally, the growing attack surface in distributed environments is addressed by expanding the scope of the hybrid approach to include edge computing and Internet of Things (IoT) devices. The rise of IoT and edge computing brings new security challenges, but introducing hybrids can provide complete security protection over complex infrastructure types. These advancements can help pave the way to a complete and responsive security strategy that will be appropriate for tomorrow's cloud ecosystem.

## XI. REFERENCES


[1] Deb, M., & Choudhury, A. (2021). Hybrid cloud: A new paradigm in cloud computing. Machine learning techniques and analytics for cloud security, 1-23.

[2] Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). Cloud computing security--trends and research directions. In 2011 IEEE World Congress on Services (pp. 524-531). IEEE.

[3] Radwan, T., Azer, M. A., & Abdelbaki, N. (2017). Cloud computing security: challenges and future trends. International Journal of Computer Applications in Technology, 55(2), 158-172.

[4] Paxton, N. C. (2016, November). Cloud security: a review of current issues and proposed solutions. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC) (pp. 452-455). IEEE.

[5] Zero Trust Architecture: The Future of Cybersecurity, online. https://www.linkedin.com/pulse/zero-trust-architecture-future-cybersecurity-mukund-chaudhary--glcwc

[6] Kulkarni, G., Gambhir, J., Patil, T., & Dongare, A. (2012, June). A security aspect in cloud computing. In 2012 IEEE International Conference on Computer Science and Automation Engineering (pp. 547-550). IEEE.

[7] Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In The 33rd International Convention Mipro (pp. 344-349). IEEE.

[8] What is the Cloud Maturity Model: Guide For Successful Cloud Adoption, Bacancy, online. https://www.bacancytechnology.com/blog/cloud-maturity-model

[9] Van Der Aalst, W. M. (2021). Hybrid Intelligence: to automate or not to automate is the question. International Journal of Information Systems and Project Management, 9(2), 5-20.

[10] Hagemann, S., Sünnetcioglu, A., & Stark, R. (2019). Hybrid artificial intelligence system for the design of highly automated production systems. Procedia Manufacturing, 28, 160-166.

[11] Czako, Z., Sebestyen, G., & Hangan, A. (2021). AutomaticAI–A hybrid approach for automatic artificial intelligence algorithm selection and hyperparameter tuning. Expert Systems with Applications, 182, 115225.

[12] Agarwal, A., Siddharth, S., & Bansal, P. (2016, March). Evolution of cloud computing and related security concerns. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN) (pp. 1-9). IEEE.

[13] McKay, M. (2012, May). Best practices in automation security. In 2012 IEEE-IAS/PCA 54th Cement Industry Technical Conference (pp. 1-15). IEEE.

[14] Mohammad, S. M., & Surya, L. (2018). Security automation in Information technology. International journal of creative research thoughts (IJCRT)–Volume, 6.

[15] Anwar, Z., & Campbell, R. (2008). Automated assessment of compliance with security best practices. In Critical Infrastructure Protection II 2 (pp. 173-187). Springer US.

[16] O'Grady, N. (2021). Automating security infrastructures: Practices, imaginaries, politics. Security Dialogue, 52(3), 231-248.

[17] Maddireddy, B. R., & Maddireddy, B. R. (2020). Proactive Cyber Defense: Utilising AI for Early Threat Detection and Risk Assessment. International Journal of Advanced Engineering Technologies and Innovations, 1(2), 64-83.

[18] Achieving cloud excellence with cloud maturity models, IBM, online. https://www.ibm.com/think/topics/cloud-maturity-model

[19] Celik, M. (1992). Overview of compaction data analysis techniques. Drug development and industrial pharmacy, 18(6-7), 767-810.

[20] Ramos, A., Lazar, M., Holanda Filho, R., & Rodrigues, J. J. (2017). Model-based quantitative network security metrics: A survey. IEEE Communications Surveys & Tutorials, 19(4), 2704-2734.