# Automated Conformity Verification Concept for Cloud Security

Yevhenii Martseniuk[1], Andrii Partyka[1], Oleh Harasymchuk[1], and Nataliia Korshun[2]

[1] *Lviv Polytechnic National University, 12 Stepana Bandery str., Lviv, 79000, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053*

**Abstract**

The primary objective of this research is to develop an advanced automated method for configuring and managing public cloud accounts and subscriptions on prominent platforms such as AWS, GCP, and Azure. This method involves the application of standardized configurations to ensure optimal performance and security compliance. A significant component of this methodology is the intermittent scanning of the infrastructure of these cloud accounts and subscriptions. This scanning is meticulously designed to identify and address any deviations or non-compliance issues with globally recognized security standards, including NIST 800-53, ISO 27001, HIPAA, and PCI DSS. The approach leverages cutting-edge automation technologies to streamline the deployment and management of cloud resources. By automating the application of configurations, the method aims to reduce manual effort, minimize the likelihood of human error, and enhance operational efficiency. This automation extends to the continuous monitoring and auditing processes, enabling real-time detection of configuration drifts or security vulnerabilities. Furthermore, the research delves into the development of a dynamic, responsive system capable of adapting to the evolving requirements of cloud security. The automated scanning component plays a pivotal role in this aspect, providing ongoing assurance that the cloud environments adhere to the strictest security protocols and standards. Continuous compliance monitoring is critical in today's ever-changing digital landscape, where threats to data security and privacy are increasingly sophisticated. By integrating these automated processes, the proposed method promises not only to bolster the security posture of cloud environments but also to offer a scalable, efficient solution for cloud infrastructure management. This automated approach is poised to set a new standard in cloud management, aligning with best practices in IT security and compliance, and paving the way for more secure, manageable, and efficient cloud computing practices.

**Keywords**

Hosting, security standards, automation, cloud technologies, cloud service models.

## 1. Introduction

Currently, most cloud environments require the implementation of accounting mechanisms, control of external security perimeter, cost control, and monitoring by cybersecurity specialists. In most cases, the process of applying configurations to create a cloud environment is the same and typical in the sequence of actions.

Based on this, this process can be automated to save time and money on creating something that has already been created more than once.

The main task of this work is to create a service for automatic application of configurations to create a cloud environment, its accounting in the internal accounting system of the organization, user access accounting, control by monitoring tools through logs for finances spent by cloud environment services,

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine

EMAIL: yevhenii.v.martseniuk@lpnu.ua (Y. Martseniuk); andrijp14@gmail.com (A. Partyka); garasymchuk@ukr.net (O. Harasymchuk); n.korshun@kubg.edu.ua (N. Korshun)

ORCID: 0009-0009-2289-0968 (Y. Martseniuk); 0000-0003-3037-8373 (A. Partyka); 0000-0002-8742-8872 (O. Harasymchuk); 0000-0003-2908-970X (N. Korshun)

configurations of the external security perimeter, and setting up the process of control over critical vulnerabilities and non-compliances with security standards by cybersecurity specialists [1].

Cloud security is a critical aspect of modern information technology infrastructure, particularly in the context of the increasing reliance on cloud computing for both business and personal applications [2].

The technologies in cloud computing have their security solutions but these solutions are provided only from the provider side, and this is a drawback for the existing security system in cloud computing. The customer or Organization does not have any knowledge of where its data is stored and also, it does not have access and control to the status of data. Each transaction is controlled by the server (or provider) side [3].

Building IT services on public cloud infrastructure highlights the necessity of precise control and visibility over highly dynamic environments.

Cloud services that become a part of business applications and development processes cannot be managed in a legacy IT way by restricting their usage to only predefined configurations, network topologies, and statically allocated resources.

This paper focuses and proposes relies on modern tools, purpose-built to process cloud platform configuration and event streams, as well as dynamically track the security compliance, cloud configuration vulnerability, and utilization state of resources. Extensive use of orchestrated automation through platform APIs ensures a consistent view of the cloud resources and related services at any stage of the environment life cycle.

## 2. Research on Common Threats to Cloud Environment Security

The main issue with security in the cloud environment is that the responsibility for security is shared between the provider and the user. Most providers offer access to their services without enabled security controls, which is good for the process of service development but creates vulnerabilities for security and data leaks from cloud environments [4].

Data confidentiality also becomes increasingly important for users and government institutions. According to the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), organizations must collect information transparently and implement policies that help prevent data theft or misuse [5–7]. Non-compliance with these requirements can lead to significant losses and damage to the organization's reputation [8].

Organizations use cloud computing and cloud-based collaboration or messaging tools to share files and information with colleagues and partners. At the same time, they can put regulated data and Intellectual Property (IP), such as trade secrets, engineering designs, and other sensitive corporate data, at risk.

Cloud computing infrastructure requires protection from cyber threats. Cloud security is a branch of cybersecurity devoted to this task. Not only is cloud security important for the protection of data, but it also helps industries and organizations meet compliance requirements, safeguard against reputation damages, establish business continuity in case of disruptive events, and even provide a competitive advantage in a highly cloud-based landscape [9].

Cloud security is essential in helping organizations address specific vulnerabilities and threats. Employee negligence or lack of training can create cloud security threats, such as oversharing files via public links that anyone can access. Data theft by insiders is also common. For example, salespeople leaving your company can steal data from cloud CRM services [10].

Shadow IT refers to using cloud apps and services without explicit IT approval. Users typically use unapproved Software-as-a-Service (SaaS) applications for file sharing, social media, collaboration, and web conferencing. Users who upload corporate data to unapproved apps may violate data privacy and residency regulations.

And there's another growing challenge: third-party apps and scripts with OAuth permissions. OAuth-connected third-party apps access IT-approved cloud computing services, such as Microsoft Office 365 and Google G Suite. It is common to see a hundred, if not a thousand, apps and scripts in an organization's cloud environment. Some pose risks because of poor design, giving them broader than necessary data permissions. Some are malicious or easy to exploit [11].

What's the danger of OAuth? Once an OAuth token is authorized, access to enterprise data and applications continues until revoked [12].

Based on this principle, the following key steps can be identified for organizational owners to control security:

- Identify all cloud environment providers that the organization works with and familiarize themselves with their security and privacy obligations.
- Invest in tools that provide secure access to the cloud, to monitor all applications and data used by the organization (Microsoft Azure Active Directory, AWS Identity, Google Authenticator, Okta).
- Deploy tools to manage cloud security that can detect and correct configuration errors (Prisma Cloud, Vanta).
- Implement a cloud infrastructure protection platform to integrate security measures into the development process. Regularly install updates and patches for software and implement policies to keep employee devices up to date (end-point protection).
- Implement a training process and assessment of employee awareness of the organization's security principles, so that employees are aware of the latest threats and phishing tactics [13].

Implement a protection strategy based on the 'zero trust' model and use an identity and access management system for critical infrastructure nodes.

# 3. Development of the Approach of "Continuous Automated Scanning of Configurations" as an Element of Protection of Cloud Environments

Despite the availability of numerous tools, most organizations find it difficult to effectively control access to their data and implement security policies in constantly changing cloud environments. In addition, ensuring compliance when data is stored in distributed environments creates a significant burden on specialists and already limited security teams [14].

## 3.1. What is Cloud and What Types of Offering We Have on a Market?

**IaaS, PaaS, and SaaS** are the three most popular types of cloud service offerings. They are sometimes referred to as cloud service models or cloud computing service models.

- **IaaS**, or infrastructure as a service, is on-demand access to cloud-hosted physical and virtual servers, storage, and networking—the backend IT infrastructure for running applications and workloads in the cloud.
- **PaaS**, or platform as a service, is on-demand access to a complete, ready-to-use, cloud-hosted platform for developing, running, maintaining, and managing applications.
- **SaaS**, or software as a service, is on-demand access to ready-to-use, cloud-hosted application software.

IaaS, PaaS, and SaaS are not mutually exclusive. Many mid-sized businesses use more than one, and most large enterprises use all three (Fig. 1).

'As a service' refers to the way IT assets are consumed in these offerings—and to the essential difference between cloud computing and traditional IT. In traditional IT, an organization consumes IT assets—hardware, system software, development tools, applications—by purchasing them, installing them, managing them, and maintaining them in its own on-premises data center. In cloud computing, the cloud service provider owns, manages, and maintains the assets; the customer consumes them via an Internet connection and pays for them on a subscription or pay-as-you-go basis.

So, the chief advantage of IaaS, PaaS, SaaS, or any 'as a service' solution is economic: A customer can access and scale the IT capabilities it needs for a predictable cost, without the expense and overhead of purchasing and maintaining everything in its data center. However, there are additional advantages specific to each of these solutions [15].

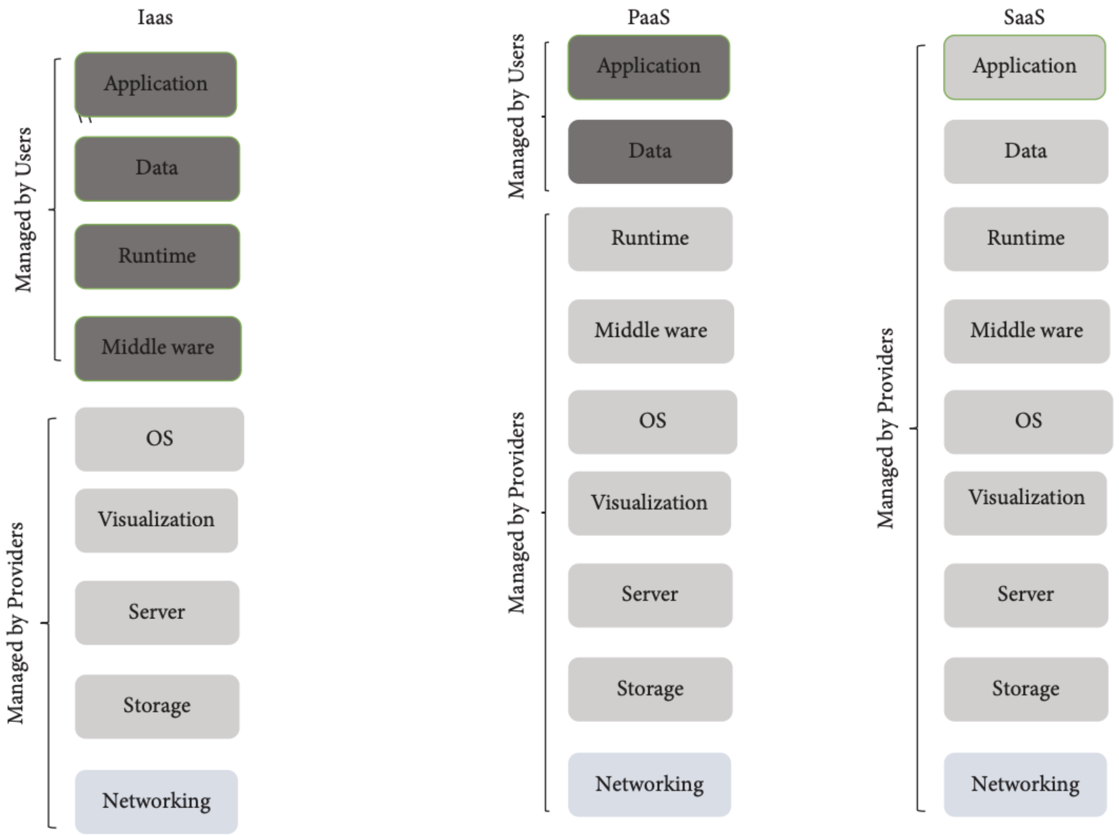

**Figure 1:** Management of resources in cloud computing

### 3.2. Continuous Automated Scanning of Configurations

The automated process uses a central orchestrator facility that performs provisioning and changes to the IaaS cloud and supporting services. It is based on the Rundeck platform and a library of scenarios composed of a well-known IT automation toolset, Ansible [16], and Python [17]. The scenarios themselves are maintained and developed within the CI development process with code control and testing.

Orchestrator and scenario structure are designed not to store any data about the cloud environments they control. All needed data for a job to perform and job status is communicated to and from Rundeck via REST API. This solution is used to ease scaling and meet requirements for system availability and security.

Security of the orchestrator when assessing cloud environments may be enhanced with storage services for secret information such as HashiCorp Vault [18].

Configuration scanning is the process of detecting inconsistencies in the configuration based on cloud environment logs (Audit logs, Flow logs) and comparing the configuration with the recommended cyber security standards (NIST 800-53, HIPAA, PCI-DSS, SOC, ISO) [19].

Using continuous integration through audit and flow logging between cloud environments and Prisma, the system ensures continuous monitoring and compliance. This integration facilitates real-time visibility into cloud infrastructure, allowing for immediate identification and rectification of any deviations from established security standards or operational benchmarks. The continuous integration approach not only enhances security but also ensures operational efficiency and reliability.

Furthermore, the system employs advanced analytics to interpret log data, providing insights into usage patterns and potential vulnerabilities. This data-driven approach enables proactive identification of security risks and operational inefficiencies. By leveraging machine learning algorithms, the system can predict potential issues based on historical data, facilitating preemptive actions to mitigate risks.

In addition to security and operational efficiency, the system's design prioritizes flexibility and adaptability. This is achieved through modular scenario architecture, allowing for quick adjustments and customization to meet evolving business needs and technological advancements. The use of Ansible and Python ensures that the system remains at the forefront of automation technology, benefiting from the wide support and continuous updates these tools receive from their respective communities.

Using continuous integration through audit and flow logging between cloud environments and Prisma Cloud, continuous control over configurations, external perimeter, costs, change management, authorization, and reduction of these assets to appropriate security standards was achieved (Fig. 2).

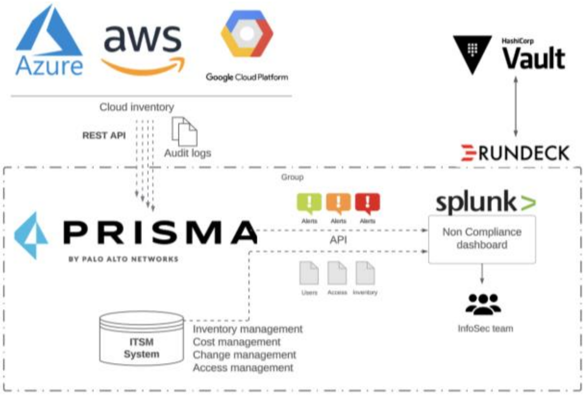

**Figure 2:** Automated scanning of configurations process diagram

## 3.3. Cost-Benefit Analysis of Automated Configuration Scanning

**Reduced Operational Costs:** One of the most significant benefits of automated configuration scanning is the reduction in operational costs. By automating routine checks and maintenance, organizations can significantly reduce the time and labor associated with manual configuration reviews. This automation translates into direct cost savings, as less staff time is required for these tasks, allowing personnel to focus on more strategic initiatives.

**Prevention of Costly Breaches:** Automated configuration scanning plays a critical role in identifying potential vulnerabilities before they can be exploited by malicious actors. The cost of a data breach or security incident can be substantial, not just in terms of financial loss but also in reputational damage. Early detection and remediation of vulnerabilities through automated scanning can prevent these costly incidents, providing a significant return on investment.

**Optimization of Resource Usage:** Automated scanning helps in identifying over-allocated or underutilized resources within the cloud environment. By optimizing these resources, organizations can achieve significant cost savings on their cloud expenditure. Efficient resource utilization not only reduces costs but also enhances the overall performance of cloud services.

**Compliance Cost Reduction:** Non-compliance with regulatory standards can result in hefty fines and legal repercussions. Automated configuration scanning ensures continuous compliance with various industry standards, thereby avoiding the costs associated with non-compliance. This continuous compliance is not only a cost-saving measure but also strengthens the organization's position in regulated industries.

**Increased System Uptime:** By maintaining optimal configuration settings, automated scanning contributes to increased system uptime and reliability. Downtime can be incredibly costly for businesses, in terms of both lost revenue and recovery expenses. The stability provided by consistent configuration scanning minimizes the risk of downtime, thus protecting against these potential losses.

**Long-term Strategic Benefits:** The adoption of automated configuration scanning aligns with long-term strategic benefits. It fosters a culture of efficiency, security, and compliance within the organization. These benefits, though not directly quantifiable in the short term, contribute to the overall health and competitiveness of the business in the long run [20].

The cost-benefit analysis of automated configuration scanning reveals a compelling case for its implementation. The upfront investment in such systems is outweighed by the substantial savings in operational costs, prevention of costly breaches, optimization of resources, reduction in compliance costs, increased system uptime, and long-term strategic benefits. This analysis underscores the importance of automated configuration scanning as a vital component in modern cloud management strategies.

## 3.4. The Benefits of the Automated Approach

**Detection of Inconsistencies:** Configuration scanning efficiently identifies discrepancies and inconsistencies in cloud settings by analyzing environment logs. This proactive detection is crucial for maintaining the integrity and security of cloud infrastructures.

**Compliance with Security Standards:** By comparing current configurations against established cybersecurity standards like NIST 800-53, HIPAA, PCI DSS, SOC, and ISO, configuration scanning ensures adherence to these critical guidelines, enhancing overall security compliance.

**Continuous Integration and Monitoring:** The integration of configuration scanning within the Continuous Integration (CI) process, using tools like Ansible, Python, and Prisma Cloud, allows for ongoing monitoring and control over cloud configurations. This continuous approach is key to maintaining secure and efficient cloud environments.

**Improved Security Posture:** With the use of advanced tools and techniques, including audit and flow logging, the scanning process contributes to a stronger security posture by managing the external perimeter, monitoring costs, and overseeing change management and authorization processes.

**Enhanced Data Security:** The use of services like HashiCorp Vault for storing sensitive information, and the design of orchestrators to not store cloud environment data directly, reinforces the security of the configuration scanning process, ensuring that sensitive data remains protected.

**Scalability and Reliability:** The configuration scanning system is designed for scalability and high availability. The use of REST API with Rundeck for communication ensures that the system can scale effectively while meeting stringent security and availability requirements.

## 3.5. Why is it Important?

Configuration scanning plays a vital role in cloud environment management by ensuring adherence to critical cybersecurity standards, detecting vulnerabilities and risks early for prompt remediation, maintaining the overall integrity and reliability of the system, providing continuous monitoring in dynamic cloud settings, facilitating thorough audit and compliance processes, enhancing operational efficiency through automation, reducing associated manual checks and potential downtime costs, and significantly bolstering customer and stakeholder trust through a demonstrable commitment to data security and privacy. Moreover, in safeguarding against evolving cyber threats. With the ever-changing landscape of cybersecurity risks, proactive scanning allows organizations to stay ahead of potential threats by identifying and addressing security gaps before they can be exploited. This proactive stance is crucial at a time when cyberattacks are becoming more sophisticated and frequent.

In addition to security benefits, configuration scanning greatly aids in resource optimization and cost management. Continuously analyzing cloud environments, helps identify underutilized or inefficiently configured resources, enabling organizations to optimize their cloud spend and resource allocation. This financial prudence is especially important in large-scale cloud deployments, where unchecked resource usage can lead to significant unnecessary expenses.

Another key aspect is its role in ensuring regulatory compliance. With increasing regulatory demands, especially in industries handling sensitive data, configuration scanning ensures that cloud environments comply with regulations such as GDPR, HIPAA, and others. This compliance is not just a legal necessity but also an ethical obligation to protect user data, reinforcing the organization's reputation in the market. Furthermore, configuration scanning contributes to a more streamlined and agile IT workflow. By automating the detection and reporting of configuration issues, IT teams can focus on more strategic tasks rather than being bogged down by routine checks. This shift towards a more strategic focus is integral in driving innovation and staying competitive in the digital landscape.

Lastly, configuration scanning enhances disaster recovery preparedness. By regularly checking and ensuring that cloud environments are configured correctly, organizations can ensure faster recovery times in the event of a disaster. This preparedness is essential for maintaining business continuity and minimizing the impact of any unforeseen events. In conclusion, configuration scanning is not just a technical necessity but a strategic asset in cloud environment management. It plays a crucial role in cybersecurity, regulatory compliance, cost management, operational efficiency, and disaster recovery, making it an indispensable tool for organizations leveraging cloud technology.

## 3.6. Components That Were Used

**Prisma Cloud™** is a PaloAlto Networks product that allows you to monitor configurations, compare them with security standards, analyze the configuration of cloud services, identify risks, and perform automatic configuration corrections according to established security policies.

Automate scanning uses the specialized service—Prisma Public Cloud—to continuously inspect the configuration of cloud environments, track asset history, and monitor administrator actions. The compliance management process implemented on Prisma Public Cloud compares platform configuration to the requirements of information security standards and alerts the SIEM system about out-of-compliance cases. It also provides notifications regarding administrators' insecure actions and optional reporting on suspicious network connections that may indicate attack attempts.

Every cloud account selected for compliance inspection is configured with an access role for the Prisma Public Cloud service, including appropriate configuration and event exporting services. In this framework, a job on the Rundeck orchestrator takes this account on Prisma Public Cloud and correctly identifies it for an appropriate inspection profile.

To inspect code and processes, Prisma Public Cloud functionality can also be integrated with cloud environments on host and container levels. This capability is particularly useful in environments that require controls for the secure development of product code.

Additionally, Prisma Cloud offers enhanced visibility and control over multi-cloud environments. Its comprehensive dashboard provides a unified view of security and compliance across various cloud platforms. This holistic approach is critical for organizations operating in hybrid or multi-cloud infrastructures, where visibility can often become fragmented. Prisma Cloud features advanced threat detection capabilities. By leveraging AI and machine learning algorithms, it can detect anomalous behaviors and potential threats in real-time. This level of security intelligence is crucial for preemptively identifying and mitigating sophisticated cyber threats.

Another critical aspect of Prisma Cloud is its ability to automate remediation actions. When a security risk or compliance issue is detected, the system can automatically implement predefined remediation steps or provide recommendations for manual intervention. This automation not only speeds up the response time but also reduces the potential for human error [21].

Prisma Cloud also supports custom policy creation, allowing organizations to tailor security and compliance checks to their specific needs. This customization ensures that the security measures are not just broad and generic but are specifically aligned with the organization's unique requirements and risk profile.

**Splunk** is a company, the market leader in SIEM (Security information and event management)—a combination of two terms denoting the scope of the software: SIM (Security information management)—security information management, and SEM (Security event management)—event management security.

Every IaaS environment enrolled in an automated scanning system is typically configured to export platform events into Splunk SIEM hosted. Enrollment operation configures the appropriate access roles and event notification services on the IaaS platform side along with a dedicated Splunk index to store and visualize the event data and dashboards.

Users who are entitled to appropriate access roles within a given cloud environment might be automatically provisioned with access to Splunk dashboards for the relevant environment.

There is a data-level integration between SIEM and the ITSM platform to export Configuration Item objects that describe cloud environments and all related incidents into Splunk. This integration is aimed at enriching events that are received from cloud platforms with business-level and process-level metadata. This capability is used to implement dashboards that display incidents related to environments, their processing speed, priority classification, service impact, and more [22].

**Rundeck** is a runbook automation platform that significantly reduces and optimizes operational workflows. What characterizes it is the easy-to-use user interface that allows technical or non-technical staff to administrate and carry out complex tasks with no requirement of special training. It's this feature in fact to be particularly efficient in time-critical environments in which reduced time of response and self-reliance are a must.

The most outstanding characteristic of this platform is its ability to introduce automation into complex workflows. Designed to execute operational tasks with consistency and without errors, plays a crucial role in maintaining operational integrity and efficacy. The standardization brought into play by this solution is critical across large organizations where multiple teams working on multiple processes can often pretty easily get misaligned and lead to discrepancies. Automating these routine, complex tasks frees up valuable time for IT staff to concentrate on more strategic initiatives. This is a game changer that is done to enhance the overall output and efficiency of the team by shifting from manual, repeatable work to more value-added activities.

Rundeck also performs well to give greater control and governance of IT operations. It has a tight detailed logging feature that ensures transparency and accountability when issuing operating processes to track as part of governance. Moreover, integration with several existing tools and systems allows single operational centers to be created that will improve operations with little change. In the case of security and compliance, all operational tasks are carried out according to the set protocols and standards. Access control as well as audit trail functionalities in the platform play critical roles in maintaining an operational secure environment where there are no loopholes to any potential breaches as well as fulfilling the regulatory requirements placed on such systems [23].

**Runbook automation** refers to the use of software to automate routine, repetitive, and often complex operational tasks, and procedures within an IT environment (Fig. 3). Traditionally, a runbook is a compilation of routine procedures and operations that the system administrator or operator carries out. Automation of these runbooks means using software to execute these procedures automatically or with minimal human intervention.

Rundeck, as a runbook automation tool, enhances this process by providing a comprehensive and user-friendly platform for automating a wide array of IT tasks. It allows IT teams to codify their operational procedures into automated workflows. These workflows can range from simple, routine tasks to complex, multi-step processes. By doing so, Rundeck not only reduces the time and effort involved in executing these tasks but also minimizes the potential for human error.

One of the key features of Rundeck is its ability to integrate with a wide variety of tools and systems, making it a versatile option for many IT environments. This integration capability means that Rundeck can orchestrate complex processes across different systems, providing a cohesive operational experience [24].

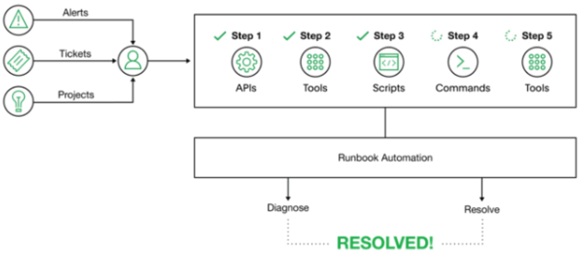

**Figure 3:** Runbook automation process

**HashiCorp Vault** is designed to help organizations manage access to secrets and transmit them safely within an organization. Secrets are defined as any form of sensitive credentials that need to be tightly controlled and monitored and can be used to unlock sensitive information. Secrets could be in the form of passwords, API keys, SSH keys, RSA tokens, or OTP. HashiCorp Vault makes it very easy to control and manage access by providing you with a unilateral interface to manage every secret in your infrastructure. Not only that, but you can also create detailed audit logs and keep track of who accessed what [25].

HashiCorp Vault is a secrets management tool specifically designed to control access to sensitive credentials in a low-trust environment. It can be used to store sensitive values and at the same time dynamically generate access for specific services/applications on lease. Plus, Vault can be used to authenticate users (machines or humans) to make sure they're authorized to access a particular file. Authentication can either be via passwords or using dynamic values to generate temporary tokens (which can be generated by pseudo-random sequence generators [26–28]) that allow you to access a particular path. Policies written using HashiCorp Configuration Language (HCL) are used to determine who gets what access.

**Secret management:** HashiCorp Vault can be used to store any type of secrets, including sensitive environment variables, database credentials, API keys, and more, giving users control over who has access and who does not. Using Vault allows you to take full control of any sensitive credentials with the ability to rotate and revoke access at any time.

With HashiCorp Vault, you can rest assured that your credentials are secure, compared to storing plaintext files in your configuration management (for example).

Instead of storing plaintext files for all the world to see, you can have your application query vault read or the HashiCorp API, which protects the plaintext versions of those files.

Secrets are also easy to rotate and revoke; if an employee leaves your organization, you can easily and securely revoke their access.

**Identity-based access:** HashiCorp Vault uses identity-based access to broker access to systems and secrets. When it comes to authenticating via identity, there are two major actors: humans and machines.

Managing access for humans is done through Role-Based Access Control (RBAC) [29], granting permission and restricting access to either create and manage secrets or manage other users' access based on the secret value they are logged in with.

Managing access for machines on the other hand involves providing access to different servers or secrets. With the dynamic nature of HashiCorp Vault, you can create secrets that work temporarily and revoke access in the event of a breach. You can generate secrets on-demand for a particular system like Sensu, AWS, or Consul and generate a key pair with valid permission. After usage, the dynamic secrets generated will be automatically revoked.

**Data encryption:** Vault provides "encryption as a service," encrypting data in transit (with TLS) and at rest (using AES 256-bit CBC encryption). This protects sensitive data from unauthorized access in two major ways: as it travels across your network as well as in storage in your cloud and data centers [30].

With centralized key management, it's straightforward to update and roll out new keys across distributed infrastructure [31].

**ITSM System**—a system of accounting for the organization's assets. Contains information about assets, projects, cost distribution, recorded changes, accounting of the authorization system, and granted accesses [32].

Any service automation and orchestration need a reliable source of records and metadata store:

- Services which they contain.
- Identification and naming of the components.
- Relation to organizational structure.
- Current state in the life cycle.
- Configuration items and dependencies that are configured

ITSM platform stores complex data structures—Configuration Items (CIs)—for every cloud account and related service elements. In the process of managing the environment life cycle, as CI records are modified (enrolling a new account, changing account ownership, or setting a monitoring profile), changes are communicated to the orchestration platform through API transactions, and respective configuration modifications are introduced to the cloud services.

Using the ITSM/CMDB system to centrally store cloud environment metadata ensures that all resources are provisioned consistently, within the required pattern, and always have actual connections to related entities.

Moreover, this centralized approach to managing cloud environment metadata via an ITSM/CMDB system is instrumental in enhancing the overall governance and control over IT resources. It allows for a structured and organized way of tracking the assets throughout their lifecycle, from procurement to decommissioning. This systematic tracking is crucial for effective asset management, ensuring that every asset is accounted for and utilized efficiently [33].

Additionally, the integration of ITSM systems with cloud services facilitates better risk management. By maintaining an up-to-date inventory of assets and their configurations, organizations can quickly identify and respond to potential security vulnerabilities or compliance issues. This proactive approach to risk management is essential in minimizing the impact of security threats and ensuring compliance with various regulatory requirements. Another key benefit of using an ITSM system in conjunction with cloud services is the improvement in incident and change management processes. With a comprehensive view of all assets and their configurations, IT teams can more effectively diagnose and resolve incidents. Furthermore, the system ensures that any changes to the IT environment are properly documented and implemented, reducing the likelihood of errors or disruptions to services [34].

The ITSM system also plays a critical role in financial management and cost optimization. By providing detailed insights into asset utilization and costs, organizations can make more informed decisions about their IT investments. This financial transparency is vital for optimizing IT spending and aligning IT resources with business objectives. In summary, the integration of ITSM systems with cloud environments brings about numerous advantages, including enhanced governance and control, improved risk management, more efficient incident and change management, and better financial oversight. These benefits underline the importance of ITSM systems in modern IT infrastructure management, especially in the context of increasingly complex and dynamic cloud environments.

**REST API** is a set of definitions and protocols for building and integrating software. It is sometimes referred to as a contract between an information provider and an information consumer that establishes the content requested by the consumer (the call) and the content requested by the producer (the response) [35].

REST is a set of architectural constraints, not a protocol or a standard. API developers can implement REST in a variety of ways.

When a client request is made via a RESTful API, it transfers a representation of the state of the resource to the requester or endpoint. This information, or representation, is delivered in one of several formats via HTTP: JSON (Javascript Object Notation), HTML, XLT, Python, PHP, or plain text. JSON is the most generally popular file format to use because, despite its name, it's language-agnostic, as well as readable by both humans and machines [36].

Something else to keep in mind: Headers and parameters are also important in the HTTP methods of a RESTful API HTTP request, as they contain important identifier information as to the request's metadata, authorization, Uniform Resource Identifier (URI), caching, cookies, and more. There are request headers and response headers, each with its own HTTP connection information and status codes.

For an API to be considered RESTful, it must conform to these criteria:

- A client-server architecture made up of clients, servers, and resources, with requests managed through HTTP.
- Stateless client-server communication, meaning no client information is stored between get requests and each request is separate and unconnected.
- Cacheable data that streamlines client-server interactions.
- A uniform interface between components so that information is transferred in a standard form. This requires that:
  - resources requested are identifiable and separate from the representations sent to the client.
  - resources can be manipulated by the client via the representation they receive because the representation contains enough information to do so.
  - self-descriptive messages returned to the client have enough information to describe how the client should process it.
  - hypertext/hypermedia is available, meaning that after accessing a resource the client should be able to use hyperlinks to find all other currently available actions they can take.

- A layered system that organizes each type of server (those responsible for security, load-balancing, etc.) involves the retrieval of requested information into hierarchies, invisible to the client.
- Code-on-demand (optional): the ability to send executable code from the server to the client when requested, extending client functionality.

The testing phase of this research project was comprehensively conducted using the infrastructures of major cloud environments, specifically Azure, AWS, and GCP. This diverse selection of platforms was instrumental in validating the versatility and effectiveness of the automated configuration and scanning method across different cloud ecosystems. Each of these cloud environments presents unique characteristics and challenges, making them ideal for a thorough and robust testing process.

In Azure, the testing focused on assessing how well the automated method integrates with its native tools and services, particularly in terms of configuration management and compliance with security standards. AWS, with its extensive service offerings and complex infrastructure, provided a broad testing ground for evaluating the scalability and adaptability of the method. The testing in GCP aimed to analyze the effectiveness of automation in a Google-centric environment, especially considering GCP's distinct security and management tools.

During the testing, various scenarios were simulated to encompass a wide range of possible configurations, security challenges, and compliance requirements. This included deploying different types of cloud resources, applying varied configuration settings, and then conducting intermittent scans to detect any non-compliance with the specified global security standards like NIST 800-53, ISO 27001, HIPAA, and PCI DSS.

The testing also involved monitoring the automated system’s response to induced configuration changes and potential security breaches. This provided valuable insights into the system’s capacity to promptly identify and rectify non-compliant configurations and vulnerabilities, thereby ensuring continuous adherence to the highest security standards.

# 4. Conclusions

In this work, a service was proposed and designed that can be used as a mechanism for continuous and automated control of accounts/subscriptions in cloud environments such as Azure (Microsoft), AWS (Amazon), and GCP (Google). The service consists of the following modules:

- Configuration Control Module: This module is responsible for ensuring that the cloud environments adhere to predefined security standards. It conducts basic checks for compliance and maintains the necessary configuration standards.
- Accounting and Audit Module: It includes components for managing user access, setting spending limits, tracking changes, and monitoring the lifespan of assets. This module is key for maintaining accurate records and ensuring financial and access-related compliance.
- Reporting and Notification Module: This module is designed to facilitate communication with cybersecurity professionals. It provides analytical tools for a comprehensive overview of various cloud environments, allowing for centralized reporting and alerting.
- Continuous Integration Tools: These are used for developing and testing scenarios within the automation approach. Tools like Ansible and Python are typically involved, allowing for flexible and efficient automation scripting and orchestration.
- Orchestrator Tool (e.g., Rundeck): Rundeck serves as the central orchestrator, handling the provisioning and management of cloud resources. It coordinates the execution of tasks and workflows as defined in the automation scenarios.
- Secrets Management (e.g., HashiCorp Vault): This module is used for securely managing and storing sensitive information like passwords, tokens, and keys, essential for enhancing the security of cloud assessments.
- Compliance and Security Standards Scanning Tools (e.g., Prisma Cloud):

These tools are used for continuous scanning of cloud configurations against recommended cybersecurity standards such as NIST 800-53, HIPAA, PCI DSS, SOC, and ISO, ensuring ongoing compliance.

Audit and Flow Logging Tools: Integral for tracking and monitoring the operations and changes within cloud environments, these tools provide the necessary data for configuration scanning and compliance checks.

## References

[1] A. Hashmi, A. Ranjan, A. Anand, Security and Compliance Management in Cloud Computing, Int. J. Adv. Studies Comput. Sci. Eng. 7(1) (2018) 47–54.

[2] V. Lakhno, et al., Management of Information Protection Based on the Integrated Implementation of Decision Support Systems, Eastern-European J. Enterprise Technologies, 5(9(89) (2017) 36–42. doi: 10.15587/1729-4061.2017. 111081.

[3] V. Susukailo, I. Opirskyy, S. Vasylyshyn, Analysis of the Attack Vectors Used by Threat Actors During the Pandemic, 15th International Conference on Computer Sciences and Information Technologies (2020) 261–264. doi: 10.1109/CSIT499 58.2020.9321897.

[4] What is cloud security? URL: https://www.microsoft.com/uk-ua/ security/business/security-101/what-is-cloud-security

[5] Z. B. Hu, V. Buriachok, V. Sokolov, Deduplication Method for Ukrainian Last Names, Medicinal Names, and Toponyms Based on Metaphone Phonetic Algorithm, Advances in Computer Science for Engineering and Education III, vol. 1247 (2020) 518–533. doi: 10.1007/978-3-030-55506-1_47.

[6] V. Buriachok, et al., Implantation of Indexing Optimization Technology for Highly Specialized Terms based on Metaphone Phonetical Algorithm, East.-Eur. J. Enterp. Technol. 5, no. 2(101) (2019) 64–71. doi: 10.15587/1729-4061.2019. 181943.

[7] S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.

[8] O. Vakhula, I. Opirskyy, O. Mykhaylova, Research on Security Challenges in Cloud Environments and Solutions Based on the Security-As-Code Approach, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 55–69.

[9] S. Kalra, K. Atal, R. Jain, Security Issues in Cloud Computing, Int. J. Comput. Appl. 167 (2017) 37-41. doi: 10.5120/ijca2017914190.

[10] S. Sreedharan, Security and Privacy Issues of Cloud Computing; Solutions and Secure Framework, IOSR J. Comput. Eng. 10 (2013) 33–37. doi: 10.9790/0661-01043337.

[11] D. Sharma, C. Dhote, M. Potey, Security-as-a-Service from Clouds: A Comprehensive Analysis, Int. J. Comput. Appl. 67 (2013) 15–18. doi: 10.5120/11374-6642.

[12] D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

[13] R. Marusenko, V. Sokolov, P. Skladannyi, Social Engineering Penetration Testing in Higher Education Institutions, Advances in Computer Science for Engineering and Education VI, vol. 181 (2023) 1132–1147.

[14] P. Chirra, V. Kumar, Multi-Cloud Networking: Investigating Strategies and Tools for Networking in Multi-Cloud Environments (2023). doi: 10.13140/RG.2.2.11542.93768.

[15] K. Parast, et al., Cloud Computing Security: A Survey on Service-based Models, Comput. Secur. 114 (2021). doi: 10.1016/j.cose.2021.102580.

[16] B. Choi, E. Medina, Setting Up an Ansible Learning Environment, Introd. Ansible Netw. Automation (2023). doi: 10.1007/978-1-4842-9624-0_4.

[17] B. Choi, Introduction to Python Network Automation: The First Journey (2021). doi: 10.1007/978-1-4842-6806-3.

[18] N. Sabharwal, S. Pandey, P. Pandey, Infrastructure-As-Code Automation Using Terraform, Packer, Vault, Nomad and Consul: Hands-on Deployment, Configuration, and Best Practices (2021). doi: 10.1007/978-1-4842-7129-2.

[19] National Institute of Standards and Technology (NIST). (Latest Update Year). "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations." URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[20] K. Edwards, J. Riis, Expected and Realized Costs and Benefits from Implementing Product Configuration Systems (2004) 216–231. doi: 10.4018/978-1-60566-260-2.CH012.

[21] J. Dawson, et al., PRISMA Archetype-Based Systematic Literature Review of Security Algorithms in the Cloud, Secur. Commun. Netw. (2023) 1–17. doi: 10.1155/2023/9210803.

[22] G. Catescu, Detecting Insider Threats Using Security Information and Event Management (SIEM) (2018). doi: 10.13140/RG.2.2.11716.99200.

[23] Spinellis, Diomidis. Service Orchestration with Rundeck, IEEE Software 31(4) (2014) 16–18. doi: 10.1109/MS.2014.92.

[24] H. Rajavaram, V. Rajula, T. Balasubramanian, Automation of Microservices Application Deployment Made Easy by Rundeck and Kubernetes, International Conference on Electronics, Computing and Communication Technologies (2019) 1–3. doi: 10.1109/CONECCT47791.2019.9012811.

[25] HashiCorp. (Latest Update Year). "Vault by HashiCorp." URL: https://www.vaultproject.io/

[26] V. Maksymovych, et al., Combined Pseudo-Random Sequence Generator for Cybersecurity, Sensors 22(24) (2022) 9700. doi: 10.3390/s22249700.

[27] V. Maksymovych, et al., Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators, Electronics 11(13) (2022) 2039. doi: 10.3390/electronics11132039.

[28] V. Maksymovych, et al., Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs, Appl. Sci. 12(3) (2022) 1519. doi: 10.3390/app12031519.

[29] T. Baumer, M. Mueller, G. Pernul, System for Cross-domain Identity Management (SCIM): Survey and Enhancement with RBAC, IEEE Access 11 (2023). doi: 10.1109/ACCESS.2023.3304270.

[30] V. Buriachok, et al., Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 2746 (2020) 23–32.

[31] P. Riti, D. Flynn, Vault HCL, Beginning HCL Programming (2021) 129–155. doi: 10.1007/978-1-4842-6634-2_7.

[32] ITSM—IT Service Management Solution of Your Business. URL: https://www.creatio.com/page/itsm-system

[33] S. Niewiadomski, G. Mzyk, ML Support for Conformity Checks in CMDB-Like Databases (2023). doi: 10.1007/978-3-031-42508-0_33.

[34] S. Maes, ITSM beyond IT. Take the service experience to new heights, IFS (2023).

[35] What is a REST API? URL: https://www.redhat.com/en/topics/api/what-is-a-rest-api

[36] B. Williams, J. Tadlock, J. Jacoby, REST API, Professional WordPress® Plugin Development 2(12) (2020). doi: 10.1002/9781119666981.ch12.