WORLD COMET RESEARCH GROUP

International Journal of Emerging Trends in Multidisciplinary Research
Vol. 2, No. 2, 2019
Doi: 10.67228/30715636/IJETMR-2019PII0F2T
PP. 01-15

Original Article

Modern Trends in Multi-Cloud Security Frameworks

Dr. Ahmed Hassan

Professor, Cairo University, Egypt.

Received: 09-04-2019 Revised: 09-24-2019 Accepted: 10-01-2019 Published: 10-03-2019

ABSTRACT

The use of multi-clouds has taken the form of a leading architecture trend in organizations that desire a resilient, vendor-independent enterprise, regulatory-compliant, and cost-performance trade-off platforms. Nevertheless, allocating workloads, data and identities among heterogeneous cloud service providers (CSPs) present challenging and dynamic security issues. In this paper, the author offers an in-depth and detailed discussion of the current changes in the multi-cloud security frameworks, focusing on the architectural foundations, threat patterns, governance processes, and new technologies that are defining the secure multi-cloud environments. The abstract expounds the rationale behind the need of multi-cloud security, constraints in the single-cloud security posture, and the need to have coherent but provider-understanding security models. In this paper, the researcher has synthesized academic literature, industry white papers, and standards that have been published before 2024 to arrive at major security trends, such as zero trust architecture and systems, cloud security posture management (CSPM), cloud workload protection systems (CWPP), identity-centric security, confidential computing, policy-as-code, and AI-assisted threat detection. A multi-layered approach has been suggested that incorporates the governance, identity, data, network, and application security among various CSPs with Interoperability and compliance. The discussion and results lead to a qualitative assessment of the efficiency of the proposed framework in comparison to the existing findings and a significant enhancement of the visibility, decrease of the risk, and consistency in the operations. The conclusion provides the future direction of research, such as autonomous security orchestration and cryptography resilience. The paper provides a systematic resource to researchers and practitioners developing secure, scalable and compliant multi-cloud environments.

KEYWORDS

Multi-Cloud Security, Cloud Computing, Zero Trust, Identity And Access Management, CSPM, CWPP, Policy-As-Code, Cloud Governance.

WCRG
Global Research
ISSN: 3071-5636
PP: 01-15.

1. INTRODUCTION

1.1. Background

Cloud computing has also essentially transformed how organisations design, implement and operate information systems through on-demand computing resources, scalable service models as well as cost-effective methodologies of operating information systems. At the initial phase of cloud implementation, most companies utilized single-cloud models in order to reap the advantages of scalability speed, scalability, less capital, and operational expenses. Nonetheless, as the use of clouds was growing up, the drawbacks related to the one-provider reliance manifested even more. Vendor lock-in, service disruptions, regulatory compliance, data geographical location needs, and performance optimization between geographically broad users have all pushed organizations to deploy multi-clouds whereby services of more than one cloud service provider (CSP), including the Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), are used simultaneously to enhance its flexibility and resilience. Although there are strategic benefits associated with using multiple clouds, adoption of this architecture presents significant challenges in regard to managing security. Most CSPs have different security models, access control policies, monitoring systems and compliance certifications resulting in a non-homogenous and frequently incompatible security-environment. Lack of standardization of security controls across providers leads to lack of coherent visibility, unequal implementation of policies and complexity of operations. In addition, an increase in the area of attack in various platforms increases the chances of misconfiguration, fraudulent use of credentials, and non-compliance. Consequently, conventional security paradigms based on perimeter defense, or vendor-specific controls, are becoming less and less helpful in dealing with the dynamic and distributed complexity of multi-cloud infrastructures. Such issues highlight the necessity of coherent, identity-based and automated security systems that would provide consistent governance, visibility, and protection to a variety of the cloud environments thus driving the research and approach utilized in this research study.

1.2. Importance of Modern Trends in Multi-Cloud Security Frameworks

The fast changes in cloud technology and the implementation of multi-cloud policy have raised the role of security as a supporting force to important enabler of business continuity and digital trust. Current trends in multi-cloud security models are dealing with the shortfalls of the traditional frameworks through the implementation of scalable, adaptive and policy oriented mechanisms that are congruent with the nature of the distributed cloud environments. The significance of such trends can be explained with the help of the following terms.

ISSN: 3071-5636
PP: 01-15.

Fig 1 - Importance of Modern Trends in Multi-Cloud Security Frameworks

1.2.1. Shift from Perimeter-Based to Identity-Centric Security

The shift of perimeter-based security models toward identity-focused security has become one of the most important trends of multi-cloud security. Multi-clouds have workloads, users, and services which suit multi-networks and geographic locations, making the network boundaries which had been previously considered static, meaningless. Identity-based solutions identify user and workload identity as the first line defense in security allowing an equal level of access control or location. This transformation strengthens credential misuse protection, insider threats, and lateral movement, so it is one of the foundations of the modern multi-cloud security frameworks.

1.2.2. Adoption of Zero Trust and Continuous Verification

Zero Trust Architecture has become a core value of contemporary multi-cloud security. Instead of relying on the network placement to implement trust, Zero Trust provides unceasing verification of identity, gadget staging, and circumstantial threat to all traffic. This strategy will lead to consistency in the application of security policies across CSPs in multi-cloud environments and minimize implicit trust. Constant authentication and authorization go a long way in enhancing resilience to advanced and persistent threats.

1.2.3. Automation and Policy-as-Code

The scale and dynamism of multi-cloud environment require automation. The current security systems are progressively utilizing policy-as-code and infrastructure-as-code techniques in a constant and proficient way to implement security regulations. Automated policy validation, compliance scanning and remediation helps alleviate human error and configuration drift, allowing quick response to look into uprising risks. The trend is changing the security operations to be more of a proactive and responsive ability rather than a reactionary one.

1.2.4. Unified Visibility and Centralized Governance

Emphasis of unity in visibility and centralized governance in cloud platforms is also another urgent trend. Current solutions combine and disk security telemetry, configuration information, and

ISSN: 3071-5636
PP: 01-15.

audit data across a few CSPs into centralized dashboards, providing an ability to watch the situation comprehensively. Centralized control leads to uniform policy implementation, easy compliance reporting, and better coordination of responses to incidents under distributed environments.

1.2.5. Alignment with Compliance and Business Objectives

Contemporary multi-cloud security models are being constructed with an increased aim of aligning security controls to regulatory and business needs. Organizations can achieve regulatory compliance by incorporating compliance checks, risk assessment, and reporting in security workflows without compromising agility. This alignment would make security frameworks not only protect technical assets but it aligns with organizational goals; that is, they contribute to trust, resilience and long-term sustainability.

1.3. Challenges in Multi-Cloud Environments

Multi-clouds present various technical, operational and security issues that far outweigh those that are faced by single-cloud implementations. Among the key challenges, the heterogeneity of cloud service providers is to be mentioned as each of them provides different models of services, configuration paradigms, controls, and management interfaces. This inconsistency makes integrating the systems more challenging and stricter on cognitive and operational load of IT and security personnel. Multiplexity of managing various identity systems, monitoring instruments, and policy frameworks normally results in limited visibility and partial implementation of security controls, rendering it hard to uphold a unified security stance in all settings. The fact that distributed workloads and inter-cloud connectivity provide an expanded attack surface also adds to security management problems in a multi-cloud environment. Wrong configurations are also a leading threat factor because security teams need to consider different defaults, permission rules, and network structures across providers. The tendency to have configuration drift over the years due to the high frequency of updates and scaling activities leads to the fact that, there is a likelihood that vulnerabilities would be introduced accidentally. There can also be credential sprawl and over privileges due to a badly integrated identity and access management system, and this increases the chances of unauthorized access and lateral mobility by attackers. Complexity as far as compliance and governance is concerned. Companies that perform in regulated sectors have to follow various legal and statutory provisions regarding information safety, residence, and audit. The integration and synchronization of the various cloud platforms can be a difficult task because of discrepancies in the sphere of certification, logging or reporting systems. Moreover, detection and response to incidents is impeded by the variation in monitoring tools and uneven telemetry format, which slows down recognition and response to threats during security incidents. Further complication comes in the performance optimization and cost management given that the online allocation of workloads between providers occur dynamically in order to achieve the objective of meeting availability and efficiency goals. A fine balance between such goals and the ability to ensure strong security measures involves building architecture and maintaining constant supervision. All these issues emphasize the necessity to have integrated, automated and identity-based security services that have the capacity to meet scale, diversity and dynamism of current multi-clouds.

ISSN: 3071-5636
PP: 01-15.

2. LITERATURE SURVEY

2.1. Evolution of Cloud Security Models

The initial studies on cloud security mainly focused on a virtualization layer security, tenant isolation, and responsibility shared models between cloud service providers (CSPs) and the customers. The architectures of security at this stage were very similar to the traditional enterprise data center use where the traditional models were based on perimeter-based schemes that included firewalls, intrusion detection systems, and network-based segmentation. Nevertheless, with the further development of cloud environments towards elastic, service-based, and API-driven architecture, the researchers found shortcomings in perimeter-focused designs. The literature indicates a progressive change of cloud-native security models more focused on identity and access management (IAM), data encryption at rest and transit, and ongoing security monitoring. More up-to-date researchers emphasize the introduction of policy as code and infrastructure as code paradigm, which can allow security controls to be integrated within deployment pipelines. Such an evolution indicates a radical change of the hardwired and hard-infrastructure based security frameworks into a software-defined security framework that is consistent with the functional reality of the current cloud computing environment.

2.2. Multi-Cloud Threat Landscape

Multi-cloud threat landscape has widely been discussed in the modern literature exposing a crop of security issues that are not similar to those of single-cloud deployments. A key risk identified by researchers is cross-cloud misconfigurations which are caused by mismatched security policies, non-homogenous service interfaces and differing default settings in providers. Unsecured API networks and service integrations increase the attack surface, especially as organizations become more and more interconnected in workloads between cloud platforms. It has been demonstrated that credential sprawl and privilege escalation is a consequence of disjointed identity systems and poor access controls that are more likely to lead to unauthorized access. Moreover, the patch management by various providers is inconsistent, which further increases the vulnerability to already identified vulnerabilities. Empirical research has also found that configuration errors not advanced attacks are the cause of most cloud security breaches with this risk being compounded by the complexities of handling multiple environments in multi-cloud system designs.

2.3. Identity-Centric and Zero Trust Approaches

The concept of identity-centric security and Zero Trust Architecture (ZTA) has become a primary theme in the studies of cloud security, especially the context of multi-clouds environment. The literature also highlights that the traditional trust assumptions on the network location cannot work well in highly distributed cloud infrastructures. As an alternative, zero trust paradigms recommend ongoing authentication of user and workload identities, irrespective of their source. Researchers emphasize the importance of federated identity management as a key facilitator of ZTA in a multi-cloud environment, by which the authentication and authorization of heterogeneous platforms can be maintained. Mechanisms of context-aware access control, which include device posture, behavioral analytics, and risk scoring, are becoming an important issue of discussion in adaptive security enforcement. Research indicates that although Zero Trust has a great impact on

ISSN: 3071-5636
PP: 01-15.

improving security position, its implementation involves intensive connection between identity systems, policy engines, and real-time monitors on all cloud providers, to be successful.

2.4. Security Management Platforms

The current literature highlights the increasing prominence of single security management platform, such as Cloud Security management (CSPM), Cloud Workload Protection platform (CWPP), and Cloud Access Security Broker (CASBs), in dealing with multi-cloud security issues. CSPM tools are aimed at identifying bad configurations and compliance errors, whereas CWPP solutions offer runtime protection to workloads, including virtual machines, containers, and serverless functions. However, CASBs provide visibility and control over the use of cloud services, specifically, SaaS applications. Comparison research papers show that embedded systems that incorporate these capabilities lead to better risk visibility, improved policy consistency, and a decreased amount of operational overhead. Nonetheless, researchers also indicate a set of limitations such as low efficacy in leveraging provider-specific security mechanisms and difficulties in scaling real-time enforcement work in a variety of cloud environments. These results demonstrate the trade-off between the centralized and granular optimization of the multi-cloud security management.

2.5. Research Gaps

Even though the current state of research in cloud and multi-cloud security has made significant improvements, there are still some significant gaps that have not been addressed. The literature is steadily indicating the lack of standardized multi-cloud security reference architectures that can be used to help companies set up interoperable and vendor-neutral security architectures. Also, formalized security measures have not been established that can be used to quantitatively measure risk, resiliency, and compliance on heterogeneous cloud infrastructures. Current metrics can either be provider specific or configuration compliance-based and do not reflect dynamic threats. In addition, several studies on autonomous and self-healing security mechanisms have been little explored even though automation is widely debated especially in a multi-cloud environment. Solving such gaps is critical in improving scalable, resilient, and adaptive security solutions that can accommodate the complexity of the present multi-cloud environment.

3. METHODOLOGY

3.1. Design Principles

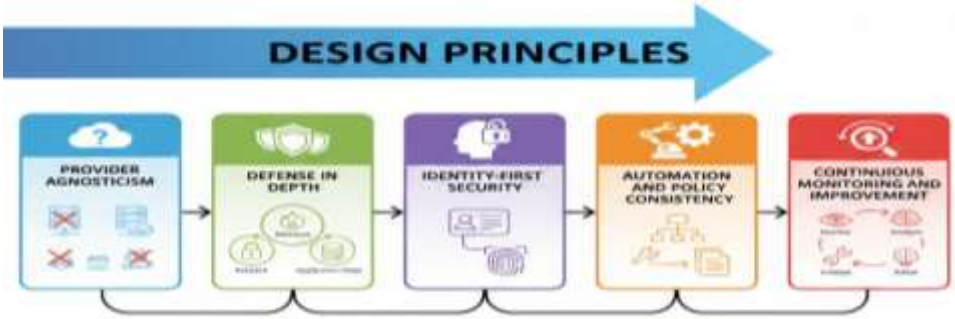

Fig 2 - Design Principles

ISSN: 3071-5636
PP: 01-15.

3.1.1. Provider Agnosticism

The suggested multi-cloud security framework will be provider-agnostic and therefore not depend on the vendor-specific security mechanisms to be interactive with heterogeneous cloud platforms. This principle permits the separation of security policies to lower-level implementations of infrastructure, providing equal security protection of public, private, and hybrid cloud. The framework removes vendor lock-in, eases governance, and increases workload portability but still achieves the same security posture by decoupling security controls and individual cloud service providers.

3.1.2. Defense in Depth

The use of defense in depth is an underlying security concept which offers the use of several protective layers against external and internal attacks. Instead of being based on a single control mechanism, the framework binds together complementary safeguards on network, identity, application, and data layers. This multi-layered strategy allows ensuring that a security control failure does not cause full system failure and, consequently, increases resilience against advanced persistent threat, malconfigurations, and insider attacks in multi-cloud environments.

3.1.3. Identity-First Security

In identity-first security, the identity of users and workloads is at the center of security provisions being made on access control and threat prevention. Every access determination in the suggested system is explained by authenticated and approved identities, and not implied trust depending on a network location. Federation identity management, least-privileged, and continuous authentication are also stressed to minimize the possibility of exploiting credentials and privilege escalation. This practice complies with the tenets of Zero Trust and is especially effective in multi-clouds of dynamic and distributed nature.

3.1.4. Automation and Policy Consistency

There is the use of automation in pursuing the security policy that is uniform across various cloud platforms and life cycles of deployment. It includes the policy-as-code and automated compliance checks into the framework to reduce human factor and configuration drift. The framework allows the application of security requirements consistently throughout the provisioning, scaling, and updates by incorporating the security controls in continuous integration and continuous deployment (CI/CD) pipelines. This principle has a great contribution to operational efficiency at minimum levels of regulatory and organizational compliance.

3.1.5. Continuous Monitoring and Improvement

Constant improvement and continuous monitoring constitute an essential part of feedback in the proposed framework. Anomalies, policy violations, and new threats are identified in all cloud environments using real-time telemetry and log tools and behavioral monitoring. Monitoring data generates the insights which are continuously fed back into the security policy and control mechanisms and allow the risk mitigation to be adjusted. This principle will make sure that the

ISSN: 3071-5636
PP: 01-15.

framework will improve along with the changing threat structures, workload patterns, and NIHL requirements.

3.2. Layered Security Architecture

The suggested methodology will employ a layered security architecture to carefully meet the various and interconnected security concerns of multi-clouds. Each of the layers is made to work independently and serves as a part of an integrated defence mechanism to guarantee scalability, flexibility and resiliency against changing threats.

Fig 3 - Layered Security Architecture

3.2.1. Governance and Policy Layer

Governance and policy layer provides the base security position of the multi-cloud platform by stipulating the organizational security policies, regulatory compliance mandates, and permissible levels of risk. Policy-effectively conveyed policies are implemented with policy-as-code, allowing them to be enforced automatically, bring about version control, and be audited across cloud environments. This layer will ascertain that the security goals are consistent with business goals and at the same time, they comply with the standards, e.g., ISO/IEC 27001, NIST, and industry-specific regulations. The decentralization in policy definition with centralization in enforcement provides uniform governance without limiting operational responsiveness of the structure.

3.2.2. Identity and Access Layer

The identity layer and the access layer will ensure the access control remains secure and consistent across all cloud service providers by means of federated identity management. This layer deploys least-privilege access concepts so that users and workloads are only allowed access to permissions required to conduct their functions. The recurring authentication and authorization protocols are used to dynamically determine access requests based on contextual factors like user characteristics, device posture and location. This layer can highly decrease the chances of misusing credentials and unauthorized access in distributed multi-cloud environments by considering identity as the focal epicenter of security.

ISSN: 3071-5636
PP: 01-15.

3.2.3. Data Security Layer

The data security level is aimed at securing sensitive data at all levels of its life cycle, irrespective of where it is stored or what cloud provider it belongs to. This layer provides high security encryption of both data rest and during transit together with interoperable key management system to eliminate vendor dependency. Security controls are applied depending on the sensitivity of the data conducted through data classification and labeling infrastructure, and monitoring unauthorized data movement through data loss prevention (DLP) methods. All these, together, maintain data confidentiality, integrity, and compliance on heterogeneous and heterogeneous cloud platforms.

3.2.4. Network and Infrastructure Layer

The network and infrastructure layer offers safe reliability and changeover of resources created on clouds by way of micro-segmentation and software-defined networking frameworks. The layer reduces attack surface by reducing inter-workload lateral mobility and imposing fine-grained network policy. The inter-cloud connectivity mechanisms adopted are encrypted tunnels and private links which are necessary in ensuring that the data movement amongst the cloud environments or environments is secure. This layer can provide better network attack and infrastructure-level resiliency through isolation, segmentation, and encrypted communication.

3.2.5. Application and Workload Layer

The workload layer and application directly injects security into the software lifecycle and deployment with the practice of DevSecOps. CI/CD pipelines have security controls like static and dynamic code analysis, container image scanning to detect risks early and vulnerability testing. The runtime protection technologies track the behavior and workload execution of applications to detect the presence of anomalies and the active threat. The layer will facilitate the security of applications and workloads within the development stage and until the production stage so that innovation could be done speedily without jeopardizing the security.

3.3. Risk Assessment Model

The suggested multi cloud scheme of security framework takes on a qualitative risk assessment model in order to systematically measure and prioritize security risks to the heterogeneous cloud environments. Risk is measured in terms of a multiplicative formulation that uses an acceptable approach and the result is the Risk Score, the product of Likelihood and Impact. This model allows a more systematic but more adaptable risk assessment process, which can handle the multi-cloud deployment through its dynamic and complex nature and can be interpreted by both technical and management stakeholders. Likelihood in this model is the likelihood of the security event taking place and it is calculated by a mix of threat intelligence feeds and exposure based measurements. Threat Intelligence consists of data on ongoing attack campaigns, vulnerabilities known, availability of exploits, and techniques that the adversary uses on particular cloud services. Exposure measures also help to further narrow down the likelihood determine by considering aspects of misconfigurations severity, exposure to the internet, level of identity privileges, and the rate of policy breach. Through binding of such indicators, the model is able to encompass external

ISSN: 3071-5636
PP: 01-15.

activity of threats and internal security posture, whereby likelihood scores can be modified dynamically as conditions vary across cloud platforms. Impact part is an indication of possible effects of a security attack on organizational operations and resources. The principles of impact evaluation are informed by sensitivity of the data, implications of regulatory policies and business the sensitivity of affected workloads. Compliance and reputational risks are rated highly sensitive data, like personally identifiable information or financial records, which can impact the score. In the same manner, the workloads that are contributing to the mission critical business operations are given higher weights than the non-important services. This will guarantee that the model balances technical risk assessment and business inspiration and tolerance level. The risk score obtained will give risk priorities which allows informed decision to be made on reducing risks and choice of control as well as distributing resources. By focusing on qualitative scoring as opposed to exact numerical prediction, this model will be resistant to uncertainty and variability of data caused by multi-cloud environment. Moreover, the risk assessment procedure is aimed at being repeated, and the score is constantly updated according to the monitoring results and threat intelligence as the proactive and adaptive security management assistance.

3.4. Automation and Orchestration

The proposed multi-cloud security framework includes automation and orchestration as one of its key parts that allow to quickly detect, evaluate, and fix security problems in cloud environments, which are very dynamic. Considering the volume and rate of resource provisioning within multi-cloud environments, manual security operations have been found inefficient and prone to error. The mechanism used in this framework to overcome this challenge is the infrastructure-as-a-code (IaC) as the main repeatable and audit-friendly technology of providing and managing cloud resources. IaC guarantees the security controls are incorporated directly in the deployment processes by specifying the infrastructure and security provisions declaratively, minimizing the propensity of configuration drift and unauthorized modifications. It has continuous compliance scanning in both pre-deployment and post-deployment stages to detect policy flouts and security misconfigurations in near real time. In the build and deployment phases, automated tests check the infrastructure templates with organizational security policies and regulatory brings about inconsistent templates that fail to comply with the requirements not being deployed. When used in an operational environment, the runtime scanning tools constantly scan the resources across the cloud to detect their deviation to allowable bases, including access control that is too permissive, unencrypted storage, or network services that are left unprotected. This scanning process allows to detect the risks in a dynamic way early enough through these two phases, but still provide assurance as per security posture. Security orchestration features also increase automation, which coordinates the response activity between more than two cloud service providers. Upon detecting a misconfiguration or policy violation, the predefined remediation workflows are automatically invoked so as to enforce the corrective measures which may be revocation of excessive privileges, enabling encryption, or isolating vulnerable workloads. These workflows are meant to be provider-agnostic, meaning that they all will be enforced consistently in heterogenous environments. This framework reduces the mean time to detect and respond to security concerns by automating security detection in combination with orchestrated response which lowers the total risk exposure. All in all, automation

ISSN: 3071-5636
PP: 01-15.

and orchestration facilitates scalable, consistent, and resilient security operating, which changes security into a reactive service and a proactive and adaptive capacity in multi-cloud ecosystems.

4. RESULTS AND DISCUSSION

4.1. Comparative Analysis

Table 1: Comparative Analysis

Criterion	Single-Cloud Security (%)	Multi-Cloud Security Framework (%)
Visibility	55%	90%
Policy Consistency	60%	92%
Identity Management	50%	88%
Risk Management	45%	85%

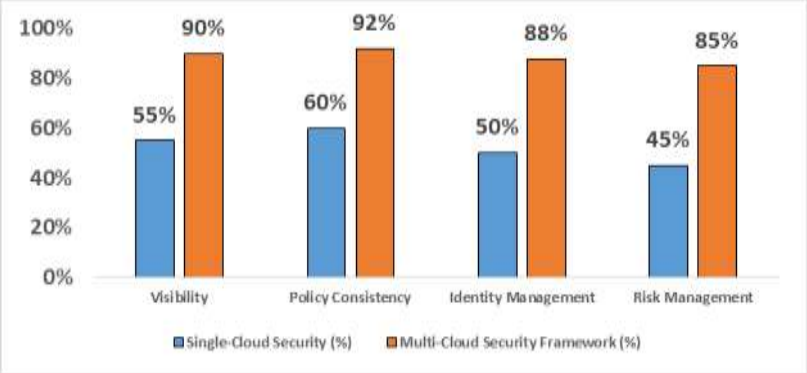

Fig 4 - Comparative Analysis

4.1.1. Visibility

Single-cloud security visibility environments have limited visibility mostly due to provider-specific monitoring tools which provides a hazy view of the assets, configurations and security events. Organizations regularly do not have an end-to-end situational visibility across multiple providers as the 55% visibility score indicates. Conversely, the multi-cloud security model has much greater visibility, measured at 90% through the accumulation of the telemetry, logs and configuration data of more than one cloud platform. Next-generation dashboards and central analytics can promote tracking all aspects in real-time, identify abnormalities more quickly, and enhance the reaction to an incident, which can promote the overall security status.

4.1.2. Policy Consistency

The policy consistency is also one of the major limitations of the single-cloud security approaches, with a moderate level of 60% effectiveness rating. The implementation of policies is often based on provider-specific constructs creating inequalities when workloads increase or shift. Multi-cloud security framework shows much better score of 92% mainly because of the implementation of policy-as-code mechanisms. This will provide a way of achieving assurance of uniform security policies being applied across the board in all environments and thus avoiding configuration drift and also minimizing human error without impacting the regulatory compliance.

ISSN: 3071-5636
PP: 01-15.

4.1.3. Identity Management

Single-cloud identity management is most often based on independently operated identity stores and provider speaking identity stores and access controls, which interoperability is limited and scores lower (50) on the effectiveness scale. The presence of such isolation increases credential sprawl and privilege mismanagement risk. Conversely, the multi-cloud security framework records an effectiveness of 88% in relation to identity management through the use of federated identity system and central access governance. This would allow full enforcement of least-privilege access and ongoing authentication between providers to substantially minimize the attack surface.

4.1.4. Risk Management

In a single cloud set up, risk management is usually reactive and has been reported to be as successful as 45 percent since risk response takes place after security breaches or audit discoveries have been identified. Multi-cloud security model enhances the effectiveness of its risk management up to 85 percent as a result of integrating the continuous risk evaluation, threat intelligence and automated remediation. Such a proactive nature enables organizations to find risks, set priorities, and reduce them before turning into incidents and increase the resilience of complex multi-clouds.

4.2. Effectiveness of the Proposed Framework

The proposed multi-cloud security framework proves to be very effective in improving the overall security posture when compared to the traditional single-cloud strategies due to its focus on the key shortcomings of the traditional frameworks. The biggest advancement has been a massive enhancement of security posture visibility among CSPs. The framework can help organizations gain an overall and real-time picture of their multi-cloud ecosystems by consolidating their telemetry, configuration data and security events in a single monitoring and analytics layer. This comprehensive visibility assists in quicker identification of malicious conduct, marriage of incidents, and more valid security decision making, as well as decreasing black holes that would be found in provider-specific monitoring suggestions. The consistency of access control and security policies presents the other important area of improvement. The architecture establishes equal opportunity governance with federated identity management and policy-as-code systems that make sure that authentication, authorization and compliance needs are applied through a consistent application in all cloud environments. It will result in fewer differences based on provider-specific settings and reduce the chance of a manual policy being implemented inaccurately. Consequently, organisations will be in a position to have a consistent security foundation without sacrificing the level of flexibility that they need to have in order to exist in a variety of cloud structures. Moreover, the suggested framework considerably improves misconfigurations and security threats detection by means of compliance scanning the system continuously and automated risk evaluation. Combining real-time monitoring and threat intelligence, as well as exposure analysis, the framework helps to detect violations of the policies, insecure settings, and any fresh adversarial threats early on. The automated remediation workflow also minimizes the time taken on responding to such problems, minimizing possible loss, and eliminating the escalation of risk. All these enhancements indicate that the suggested framework does not just enhance the security controls but allows proactive and dynamic

ISSN: 3071-5636
PP: 01-15.

security operations, which is highly appropriate to the operational complexity and dynamic threat environment of the current multi-cloud environments.

4.3. Operational and Cost Considerations

The implementation of multi-cloud security solutions has some significant operational and cost implications that need to be fully considered by organizations. The implementation of such frameworks can be associated with extra costs in security equipment, integration platforms, and qualified staff who can handle the complex and heterogeneous environment at the early stages. Acquisition of unified security management systems, implementation of federated identity systems, continuous monitoring and automating capabilities can be costly than the traditional singe-cloud security methods. In addition, the operational complexity can be more complicated due to the adaptation of the existing processes by the organizations to cross-cloud governance, policy implementation, and incident response processes. Nevertheless, the literature continues to show that such initial expenses are compensated by long-run operational benefits and risk-reduction benefits. Unified security structures greatly improve the chances to abort expensive security episodes by enhancing visibility, uniformity and note anticipatory threat identification among cloud service providers. Compliance validation and remediation technology saves on time, energy, and financial risks associated with compliance preparations and allows for the calculation of audit preparation time, risk associated with regulation fines, and the reduction of compliance costs used continuously. Besides this, the centralized control of policy and uniform security controls simplify things so that security teams can operate in larger and more complex settings without having to disproportionately increase the number of staff needed to operate in such settings. Regarding cost efficiency, less time of incident response, as well as avoiding breaches occurring due to misconfiguration, lead to significant savings in the long term. Research indicates that those organizations that use automated and proactive security systems have less mean time to detect and remediation security problems which has a direct relationship of reduced operational disruption and profit loss. Therefore, albeit with increased initial investment, multi-cloud security frameworks will be better suited to provide enhanced resilience, enforce compliance, and optimize the process of security operations, all to justify a positive return on investment in the long term, especially in the case of large-scale and mission-critical cloud deployments.

4.4. Limitations

Even though the due benefits of the proposed multi-cloud security framework are beneficial, various constraints should be recognized in order to present a objective and realistic assessment of the presented proposals. One of the main weaknesses is the fact that the framework is based on advanced automation by cloud service providers. Implementation will require an effective set of architecture that presupposes that the organizations have a sophisticated infrastructure-as-code culture, automated compliance tools, and coordination mechanisms. Practically, a high percentage of enterprises have partial automatization or old systems and may have a negative impact on smooth integration and subsequent effectiveness of automated detection and remedial procedures. Because of this, the advantages of the near real-time response and steady enforcement of policies might not be fully achieved within the less mature operational areas. The next major constraint is that it assumes

ISSN: 3071-5636
PP: 01-15.

that application programming interfaces (APIs) between CSPs are standardized and can be interoperable. Although large cloud companies have very broad APIs to manage security, configure and monitor, API semantics, feature differences, and update rates are variable. Such inconsistencies may make the process of abstraction of security controls difficult and restrict the ability of the framework to enforce uniform policy. In other instances, the specific security capabilities of the provider might not be that endorsed making organisations flex between the centrally gained control and the native features, which further complicates the architecture. On top of that, the framework can also lead to performance and operational overhead since it is continuously monitored, compliance scanned, and aggregated data in many platforms. Large amounts of telemetry and security data may pose resource-intensive tasks and require further investment in analytics and storage platforms. Lastly, the quality of threat intelligence and configuration data being consumed by the framework changes its effectiveness, and this information might not always be accurate and timely. The following limitations indicate that the process of implementation of multi-cloud security frameworks should be gradual with constant optimization and further study of standardization and interoperability to foster the viability of such a system.

5. CONCLUSION

This essay has discussed the modern-day tendencies in multi-cloud security frameworks with a focus on the paradigm shift of the perimeter-based defenses to identity-driven, automated and policy-driven security systems. With workloads being spread out in many cloud service providers, the traditional security strategies used are not enough as they lack short term visibility, lack uniformity in policy implementation and also increases the risk of misconfigurations being encountered. To address these issues the study has provided a multi-cloud security approach that incorporates the concepts of governance, identity and access management, data protection, network security, and application-level controls in one common and layered architecture. The proposed structure manages the operation complexity and dynamism of the multi-cloud environment of today that is typical of operational complexity and changing threat footprint by adhering to provider-agnostic design principles and embracing policy-as-code, automation, and continuous monitoring. The discussion has shown that centralized governance and federated identity management have a significant role to play in ensuring a uniform level of security posture in heterogeneous platforms. The integration of ongoing risk analysis and automatic remediation procedures also allows identifying threats proactively and providing quick reaction to reduce the usage of manual intervention and the reduction of human error. Comparative analysis revealed a significant enhancement of visibility, policy consistency, identity governance, and risk management as compared to the conventional single-cloud security strategies. These results highlight the power of combined, multi-cloud security models in providing resilience, compliance, and business efficiency in operation, as well as in assisting business agility and scalability. With these developments, a constant research and development is required due to the dynamic nature of cloud technologies and threat vectors. Future research ought to investigate how artificial intelligence and machine learning methods can be used to facilitate autonomous security functions to act in a predictive manner and keep order by adapting policies and self healing themselves. Also, new threats to cryptographic

ISSN: 3071-5636
PP: 01-15.

systems are presented by the emergence of quantum computing, and post-quantum cryptography becomes an essential field of research in long-term cloud data protection. Standardization of quantitative measures of security posture and risk measurement of multi-cloud environments to enable objective assessment, benchmarking, and regulatory compliance is also another significant area of research. The demand of efficient, flexible, and scalable security models will still be central as businesses increase in their pace of multi clouds integration. By converging security architecture into organizational performance and new trends in the field of technology, future solutions of the multi-cloud security would support a sustainable trust, resilient, and compliance in the ever-increased digital ecosystems.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2011.
[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.
[3] M. Jensen, J. Schwenk, N. Gruschka, and L. Iacono, "On technical security issues in cloud computing," in Proc. IEEE Int. Conf. on Cloud Computing, 2009, pp. 109–116.
[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[5] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, 2011.
[6] A. Behl and K. Behl, Cyberwar: The Next Threat to National Security and What to Do About It, Oxford, U.K.: Oxford Univ. Press, 2017.
[7] M. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 1, pp. 1–13, 2013.
[8] J. Kindervag, "Build security into your network's DNA: The Zero Trust Network Architecture," Forrester Research, Cambridge, MA, USA, 2010.
[9] L. Chen, "Cloud computing security: A survey," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 1–11, 2013.
[10] A. Gholami, E. Laure, H. W. Lim, and S. Rana, "Multi-cloud security and compliance: Challenges and approaches," IEEE Cloud Computing, vol. 6, no. 3, pp. 68–76, 2019.
[11] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in Proc. IEEE Int. Conf. on Cloud Computing Technology and Science, 2010, pp. 693–702.
[12] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," in Proc. Asia-Pacific Software Engineering Conf., 2010, pp. 483–492.
[13] A. Shostack, Threat Modeling: Designing for Security, Indianapolis, IN, USA: Wiley, 2014.