JOURNAL OF BASIC SCIENCE AND ENGINEERING

DYNAMIC CLOUD SENTINEL FRAMEWORK (DCSF) FOR CSPM AND OPTIMAL SECURITY IN DYNAMIC CLOUD ECOSYSTEMS

G Sreenivasa Yadav
Research Scholar
Department of Computer Science and Engineering
Annamalai University
Annamalainagar – 608 002

Dr. G Karthick
Assistant Professor
Department of Computer Science and Engineering
Annamalai University
Annamalainagar – 608 002

Dr. C.H. Mukundha
Associate Professor
Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad
Telangana-501301.

Abstract **–** The current cloud enterprises are expecting a robust Cloud Security Posture Management (CSPM) in orchestrating security across cloud ecosystems. Hence, this research investigates the current CSPM platforms in streamline security assessments, automating policy enforcement, and enhanced incident response. By focusing on the dynamic nature of cloud environments, the study demonstrates how CSPM acts as a sentinel, vigilantly guarding against misconfigurations and vulnerabilities. The proposed Dynamic Cloud Sentinel Framework (DCSF) includes Automated Configuration Audits (ACA), Real-Time Threat Intelligence Integration (RTII), Policy Enforcement Automation (PEA), Incident Response Orchestration (IRO), Case Study Analysis (CSA), and Continuous Improvement and Adaptation (CIA). Also through the comprehensive analysis and real-world case studies, this paper highlights the transformative power of CSPM in reinforcing cloud security. Practical insights and methodologies are presented to underscore the effectiveness of CSPM in maintaining robust security postures in ever-evolving cloud landscapes.

Keywords **–** DSCF, Dynamic Cloud Sentinel Framework, Automated Configuration Audits, ACA, Real-Time Threat Intelligence Integration, RTII, Policy Enforcement Automation, PEA, Incident Response Orchestration, IRO, Continuous Improvement and Adaptation

I. INTRODUCTION

As our digital world continues to evolve at lightning speeds, cloud computing has become of great interest to many organizations aiming to drive innovation, scalable business services, and cost savings [1]. For the industry, cloud offers limitless potential: organizations can flexibly grow and shrink their IT infrastructure and services based on business needs. Yet, the dynamic and distributed nature of cloud also exposes new threats that traditional security tools struggle to address adequately [2].

Cloud environments are inherently complex containing numerous services, configurations, and integrations across diverse platforms. Consequently, this complexity frequently results in security vulnerabilities and misconfigurations, which are primary causes of cloud-related security breaches [11][13]. Mismanaged cloud resources could reveal sensitive data, pave way to unauthorized access, and cause compliance violations [3]. Guidelines and best practices are available for organizations to follow, but enforcing consistent and continuously secure posture in dynamic cloud environments remains a daunting challenge [23-24].

Frequently, traditional approaches to security are retroactive and manual systems, not fitting the dynamic nature of cloud infrastructure [25]. Add to that the shared responsibility approach, where cloud service providers are accountable for protecting the cloud infrastructure, but organizations are responsible for the data and applications they put in the cloud, and the challenge of securing your cloud presence gets more dissimilar and much more complex. This necessitates robust and constant the security of security configuration monitoring and management, but this is resource-intensive and prone to human error [5].

In addition, the challenge is being intensified due to the exponential growth of advanced cyber threats and sophisticated attack vectors directed toward cloud environments [6-7]. Organizations are constantly plagued by determined threat actors that strive to uncover weaknesses in cloud configurations, conduct Denial of Service (DoS) attacks or compromise confidentiality of sensitive data. With the scarcity of real-time threat intelligence and automation due to automated incident response mechanisms in most organizations, the chances of conducting such attacks is very high thus leading toward severe financial and reputational damages [8].

In order to solve these critical challenges, an integrated, automated as well as dynamic security framework should be developed to supply persistent monitoring, real-time threat detection and automated response capabilities [9-10]. In this context, Dynamic Cloud Sentinel Framework (DCSF) is put forward as a comprehensive approach to orchestrate security excellence across cloud ecosystems. DCSF endeavours to simplify security evaluation, automate policy enforcement, and improve incident response, as well as forever adaptive to both emerging threats and technology advancements.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

PROBLEM STATEMENT

As the digital landscape rapidly changes, corporations have begun to adopt cloud computing to maximize scalability, innovation, and optimal operation. The cloud environment's degree of scalability and cost-effectiveness are unequalled, giving corporations the ability to expand infrastructure on demand. Nonetheless, with multiple entities in cloud computing and the ability for any application to store data, cloud computing is not without new security concerns [11-13].

Cloud environments are inherently intricate, with countless services, settings, and interfaces spread across multiple different platforms [26-27]. It's this intricacy that often results in security flaws and misconfigurations, which are among the primary causes of cloud-related security incidents. Misconfiguring cloud-reliant assets can put sensitive data within reach of attackers, open another door to unauthorized access, and invite countless potential compliance violations [14].

Conventional defense methods are frequently sluggish and hands-on, consequently powerless to respond quickly enough to the swiftly advancing world of cloud infrastructure [28]. It worsens when one takes into consideration the shared duty in cloud security model. Cloud service providers are the ones to guarantee the safety of the infrastructure, while it is our duty to keep data and applications within the cloud secure, the responsibility relies solely on us, hence making this method convoluted; making us need to continuously observe and maintain the security configurations [5].

Moreover, the surge in cutting-edge cyber threats and complex attack paths aimed at cloud infrastructures intensifies the problem. Enterprises are persistently menaced by adversaries wishing to take advantage of cloud configuration weaknesses, initiate Denial-of-Service actions, and pilfer classified databases. Without up-to-the-minute threat Intel and quick response settings in place, most enterprises are defenceless, often resulting in substantial monetary and brand image losses.

In order to deal with these security issues, an incorporated, automated, and dynamic security framework is seriously needed. This framework should provide ceaseless monitoring, real-time detection of attacks, and capacities for incident response. To address the mentioned issues, this paper proposes Dynamic Cloud Sentinel Framework (DCSF).

OBJECTIVE OF THIS RESEARCH

The primary objective of the proposed DCSF is to integrate several key components to provide a comprehensive, dynamic approach to cloud security management. Firstly, DCSF applies automated configuration audits to detect and fix misconfigurations in real-time. Secondly, while threats continue to evolve in the cloud arena, it is essential for DCSF to integrate real-time threat intelligence, or RTII, to detect and suppress emerging threats in their incubation period.Further, DCSF uses Terraform for policy enforcement automation (PEA), offering standardized, automated

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

security best practice conformity. In addition, DCSF focuses towards organizing automated incident response workflows (IRO) to decrease the effect of security incidents. To support continuous improvement, the framework employs tools for data visualization and analysis to perform case study analysis (CSA), generate actionable insights, and intuitive dashboards. Finally, it uses next-gen analytics and ML platforms to perform continuous improvement and adaptation (CIA) to emerging threats, raise the overall security posture.

MOTIVATION

The main reason for proposing DCSF is to handle and guard dynamic cloud environments. Cloud platforms are elastic where you can stretch and shrink the resources where they allow to change the amount of resources used very rapidly [29]. Additionally, the sophistication of cloud computing demands the constant improvement and adapt the security operations to keep pace with the evolution of threats in cloud environments. Conventional conservative posture against APTs, zero-day exploits, and any advanced threats or actors is no longer acceptable. Static security measures instantly grow outdated in light of new attack vector [15-16]. Traditional security solutions, in fact, provide reactive countermeasures, and react after to an event is occurred and visible [17]. Furthermore, cloud infrastructures are increasingly exposed to threats that are more and more sophisticated. This fact has highlighted the strategic importance of an integrated, proactive security approach, to account the mentioned security issues. Hence in this research a novel framework is proposed to address all the mentioned issues.

CONTRIBUTIONS IN THIS PAPER

- DCSF integrates automated configuration audits, real-time threat intelligence, policy enforcement automation, incident response orchestration, and continuous improvement mechanisms to provide a robust and dynamic approach to cloud security management. Demonstration of DCSF's efficacy through the practical implementation of real-world tools within existing cloud environments.
- Provision of actionable insights and empirical evidence through case study analysis and intuitive dashboards, effectively bridging the gap between theoretical constructs and practical execution in cloud security.
- Detailed evaluation of DCSF's performance in various attack scenarios, showcasing its ability to adapt to emerging threats and continuously enhance security measures, thereby validating its role as a proactive and adaptive security solution for cloud ecosystems.

II. LITERATURE SURVEY

The use of cloud computing has completely changed how people and all type of businesses handle and use their computing resources by offering many advantages [18-19]. Some of these advantages include: flexibility, scalability, and cost effectiveness and efficiency. Nonetheless, just as enterprises and organizations use cloud computing to store and deliver confidential and sensitive data, an expansion of concerns has developed around about safeguarding information's security in

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

this embodied realm. Achieving confidentiality and data integrity and effective data transmission has become a major challenge today. Our proposed approach addresses this concern by integrating encryption and compression techniques to improve the transmission performance in cloud and preventing unauthorized access to confidential information. Several robust encryption algorithms are employed in multiple levels in this application followed by LZMA. It reduces data size effectively, and it is secure. It is good for real-time deployment and has the performance of high encryption and compression. It has various types of performance measurement methods it helps to measure it's performance like as space saving percentage, process time, NIST randomness test. Their approach significantly improves space saving percentage from 58.63% to 81.8%, so improve the efficiency. The security analysis of cipher texts generated by our approach satisfies all the NIST standard tests and produces 99% confidence level that the plaintext is sufficiently random. The approach that is being suggested uses a combination of different techniques which will help to ensure that the sensitive data can be processed securely, meanwhile still allows it to take advantage of the resources which the cloud computing environments provide, in this particular case [1].

Authors from [2] attempted a work on cloud enabled 6G networks which presented a significant opportunity for smart cities to advance with the promise of higher throughput, lower latency and better response times. With the growth of IoT and connected devices within the smart city environment attackers have more opportunities to probe, attack, and exploit these devices for variety of malicious goals. In this paper, we propose a novel defense technique that creates a cloud-based virtualized honeypot/twin designed to receive the malicious traffic in an edge based machine learning enabled detection system. Our proposed system performs early detection of the malicious traffic in the SDN enabled edge routing point, thus deflecting the traffic flow away from 6G enabled smart city end points. The evaluation of our proposed system demonstrated an accuracy greater than 99.8% with an F1 score of 0.9984 [2].

Another paper by [3] offers a synopsis of IoT – Internet of Things with stress on important enablers, communication protocols and application issues. At its core, IoT is applied to tackle problems related to RFID and primarily to smart sensors; thus, this paper will concentrate on RFID and sensors. The primary design goal of IoT is to realize the pure object to object collaborative smart sensors, without human cognizance, to deliver the so-called Super Applications. Right now, the revolution in Internet, mobile, and machine-to-machine (M2M) technologies is connected with the first phase of the IoT. In the next few years, the IoT will connect various technologies together to offer new applications that will make up a unified system, connecting physical objects in support of intelligent decision making.In their paper, they begin by giving a horizontal overview of IoT introduction. Then they gave an overview of the technical details of IoT, focusing on the communication protocols and application solutions. Unlike other survey papers, their intention is to give a thorough summary of the mostly related communication protocols and application issues to provide researchers and application developers who are interested in this field a bird's-eye

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

overview and will not need to go through all the specifications or RFCs to figure out the protocols they will use and survey for application functionalities that they intend to support. They additionally presented a review of a portion of the key IoT challenges featured in the writing. Additionally, they give a summary of pertinent research work. In addition, they examine the association between IoT and other rising advancements including big data analytics and cloud and fog computing. Additionally, they present the need for better flat integration between IoT services [3].

Another research by [4] focuses on adoption of Industrial Internet of Things (IIoT) devices and the recent advent of edge private cloud systems to accommodate industrial settings' requirements for high data rates, low latency, and robust computing and storage capabilities, system security has quickly become a critically important issue. The early identification of attacks poses challenges for many existing machine learning-based attack detection models for the IIoT due to the heterogeneous, high-dimensional and unbalanced nature of network traffic and physical process data. Furthermore, these models are frequently trained offline and then deployed in the cloud or embedded in devices, causing resource burden and delaying attack detection. Therefore, the article introduces a real-time security model for attack detection up to security impact mitigation employing Digital Twin and online ensemble machine learning. Using gas pipeline and X-IIoTID datasets we investigate various ensemble techniques and their algorithms and assess their output. The results of the experiments exhibit a strong attack detection capability of the proposed model indicating comparative performance to offline ensemble techniques [4].

Authors from [9] fully focusses on the information security part of cloud environment. Their idea Remote Data Auditing (RDA) with Key Exposure Resilience support offers a solution for ensuring secured cloud data storage outsourced both in advance and after the key exposures. However, most of current solutions would suffer from the security attack during key-exposed interval that the cloud server is capable of discarding or tampering file from the data owner. Some others assume a secure channel for key update [5-7], which is unrealistically expensive scenario under key-exposure scenarios. In this paper, we construct an online/offline RDA framework with strong key-exposure resilience, called S-OORDA, which can resist strong key-exposure attacks and efficiently achieve the integrity verification for cloud data. Subsequently, we portray a real concrete S-OORDA scheme that enables the data possessor to advance the secret key while the secure channel existence is not necessary. Furthermore, the authenticators can be frequently updated remotely to guarantee that the unauthorized attackers do not spoof the authenticators utilizing the exposed auditing secret keys. In addition, the new spot-checking-based MDP was designed server-aided to maintain each dimension of the security in the outsourced data. Meanwhile, the data auditing process of the proposed scheme is divided to online and offline phases, greatly relieving both data owner and third-party auditor of the online computational burden. Security and performance analysis confirm that the proposed scheme meets the desired security and has the optimized efficiency [9].

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Conventional security measures are often insufficient when it comes to safeguarding against the advanced threats and vulnerabilities that exist in cloud infrastructures [20-22]. The DCSF provides a completed and adaptive set up for managing and mitigating risks proactively, with automated configuration audits, real-time threat intelligence, policy enforcement automation and incident response Orchestration to identify, manage and mitigate risks associated with the compromise of AWS resources. Combining world's best tools like ManageEngine, Wazuh, Terraform, Shuffle, Prometheus, the ELK Stack etc the DCSF will help you to monitor and response continuously to any security incidents creates a robust posture of your cloud security. It will not address only current current, if a status of continuous improvements, as it is adopting machine learning and analytics which response to the emerging third consumed, so this DCSF act as a real suppressor protecting sensitive data, supporting adherence to regulatory guidelines and overall compliance and of course giving you a powerful reporting framework to respond back to the federal audit bodies.

III. THE PROPOSED DYNAMIC CLOUD SENTINEL FRAMEWORK (DCSF)

The introduction of cloud computing has brought an incredible change in the IT sector, delivering cost-effective, scalable and flexible services. Nevertheless, the characteristic of cloud paradigm presents new security concerns that necessitate dynamic and intelligent security systems to handle them. To address the above mentioned problems, this research proposes a Dynamic Cloud Sentinel Framework (DCSF) which is an innovative and solid new technique to counteract these issues by offering holistic approach in Cloud Security Posture Management (CSPM). DCSF offers a variety of innovative components that work together such as continuous security assessment, policy enforcement, incident response and ability to learn and adapt with emerging threats. Figure 1 shows the DCSF architecture.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

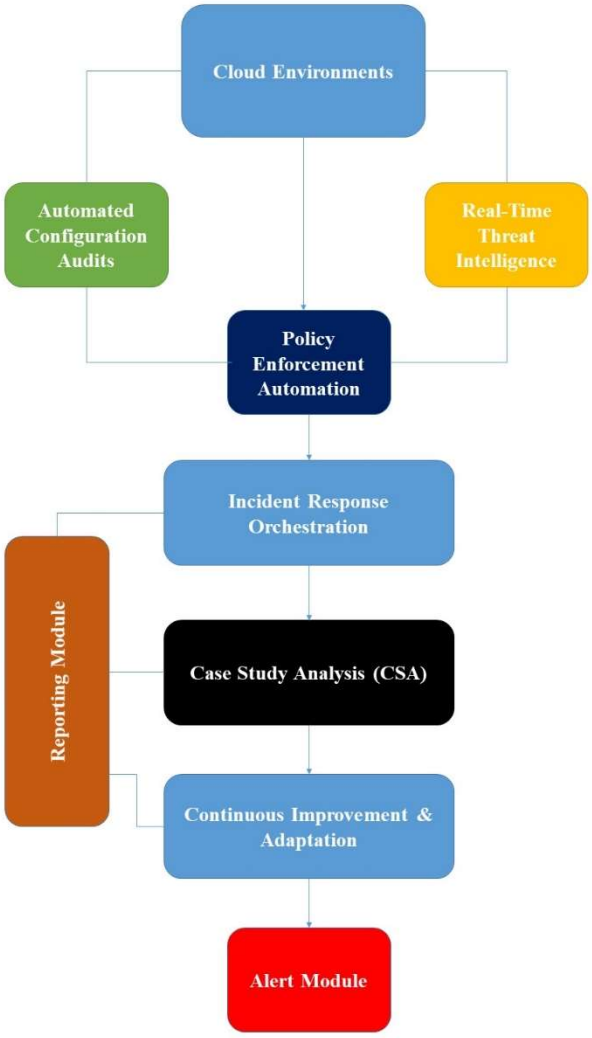

Figure 1. DCSF architecture

A. Automated Configuration Audits (ACA)

The foundation of the DCSF is the Automated Configuration Audits (ACA) which assure that the cloud configurations conform to security best practices and compliance imperatives. It runs the ACA component with state-of-the-art machine learning techniques to perform continuous and automated audits on cloud configurations. Leveraging supervised and unsupervised learning techniques, the ACA quickly identifies deviations from the established baselines configurations, as well as anomalies in the configurations, which might indicate potential security issues.

One important feature of ACA is that it is able to adapt to the particular needs of an organization. Machine learning models are trained on historical configuration data to allow the ACA component to learn what constitutes a secure configuration in a given environment. This adaptive learning means that ACA can provide recommendations that are tailored to a particular organization or environment, and also means that ACA can automatically remediate

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

misconfigurations that we find. These adaptive learning aspects distinguish ACA from many of the other audit and analysis tools that are on the market today and in fact make it a revolutionary new approach for this kind of work. Our integration with these real-time tools such as AWS Config, Azure Security Center, and Google Cloud Security Command Center also means that while ACA is performing the automated process of continuous monitoring and auditing for your cloud assets, we're not just starting from scratch with those services because ACA learns on what it has to deal with on that client's cloud assets.

Additionally, ACA applies rule-based engines to ensure industry standards and regulatory requirements are met such as GDPR, HIPAA, and PCI DSS. Through automating the verification process, ACA minimizes the manual work required for verification and guarantees policies to be applied consistently across cloud environment.

B. Real-Time Threat Intelligence Integration (RTII)

The incorporation of the latest threat intelligence streams using the Real-Time Threat Intelligence Integration (RTII) is what enhances DCSF's Cloud Security Platform Management (CSPM). Threat Intelligence information reveals where the newest attack vectors, vulnerabilities, and threat actors are, allowing organizations to handle threats that are appearing today. RTII collects the feed via an API, with the different real-time threat-intel platforms like Wazuh, ThreatConnect, Anomali, and IBM X-Force Exchange, giving it constant updates on threats. RTII also uses the state of the art data analytics and machine learning methods (which are pre-build in the platform) to match threat intelligence with cloud environment data. By cross verifying the patterns and indicators of compromise (IOCs), RTII detects the potential cloud infrastructure vulnerabilities and threats very effectively. Security teams are able to classify and target the highest-risk items before adversaries can exploit them due to the proactive method. Furthermore, RTII provides automated threat hunting and incident detection features. By consistently harnessing threat intelligence feeds and cross-referencing them with live cloud activity, suspicious patterns of behavior can be identified and alerts can be immediately generated, enabling further inquiries.

C. Policy Enforcement Automation (PEA)

The Policy Enforcement Automation (PEA) is essential to the DCSF as it guarantees that safety policies are put into effect and applied systematically throughout the cloud environment. The PEA automates it to dynamically amend security policies based on the real-time estimates of the risk and fulfilment and its requirements.

By doing so, it facilitates the ability to occasionally produce inaccuracies by human fault. It is a goal that assures that the security policies are up-to-date over the rising landscape on the sternness.

PEA comes with AWS Identity and Access Management (IAM) for AWS, Azure Policy for Microsoft Azure, and Google Cloud Identity and Access Management to enforce cloud-native security policies. By using these tools, PEA can automatically enforce vital security checks, such

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

as network segmentation, encryption, and access restrictions, based on predetermined policies and risk self-assessment.

Also, PEA supports practices such as policy-as-code which means that rules about what security policies are enabled, how they are managed and/or how they are enforced are 100% defined, managed and controlled by software. This makes them consistent and enforceable. It also means they can now be version controlled like code, it is auditable and some engineer in IT can wrap new testing models around it. Terraformis used to implement policy-as-code in DCSF.

DCSF also integrates compliance checks, regulation evaluation and feedback mechanisms. By vigilantly monitoring enforced policies' efficaciousness, collecting feedbacks from security incidents and audits, PEA can continuously adapt and hone security policies against emerging threats and vulnerabilities. The continuous improvement process guarantees the robustness and efficacy of security policies in mitigating risks.

D. Incident Response Orchestration (IRO)

The DCSF utilizes Incident Response Orchestration (IRO) to effectively and efficiently react to security threats and manage compromise in a cloud environment. IRO builds upon existing best of breed security tooling via an orchestration layer that accesses existing incident response tools and processes. By augmenting these tools with a layer of orchestration, the management of activities such as incidence detection, analysis and resolution, can be streamlined. The orchestration layer allows for tools in the DCSF to interact with tools from the cloud security providers. For example, the Cloud Agnostic Security Assurance framework (CASA) can monitor an customer implementation for movement of sensitive data that is outside of the corporate allocation. This raises an alarm in CASA which is then passed to the IRO Manager. This manager tool then performs logging of the alert and engagement into CASA, High Speed Logging, (HSL) that orchestrates the remediation activities involving CASA, a federated identity provider and the customer's workload. The whole process is logged and monitored for compliance.

IRO utilizes the pre-configured playbooks and workflows to standardize and handle the incident response. These playbooks define the process during different types of security incidents to make sure our response actions are consistent and follow the organizations policies. By automating repetitive tasks such as log analysis, threat containment and communication, IRO allows the security teams concentrate on more complex aspects of incident investigation and remediation. The DCSF has the ability to integrate with Splunk Phantom, ManageEngine UEBA and SOAR, and IBM Resilient. By integrating with these platforms, organizations can automate their incident response. These platforms offer outstanding automation and orchestration capabilities to streamline and optimize the incident response workflow for the utmost efficiency. Furthermore, IRO provides assistance with instantaneous coordinated operation and interaction among groups that are responding to accidents. IRO specifies awareness and the smooth cooperation of all stakeholders in security incidents by linking with messaging programs such as

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Slack. That real-time collaboration enriches situational awareness and allows for the quicker making of choices that thereby decreases security incident timeframes.

E. Case Study Analysis (CSA)

The CSA is an important part of DCSF that provides actual findings and confirmation of the efficiency of the structure. CSA proves through complete case studies of actual world cloud implementation how DCSF can reveal cloud configuration error detection and error recovery. These case studies analyze particular security incidents to represent how DCSF theatre can recognize and recover from the beginning cause of these incidents.

The CSA involves a full analysis of cloud environments across a range of industry and use cases. Exploring a variety of cloud architectures, configurations, and security practices, the CSA reveals a complete view of the issues and solutions surrounding cloud security. The result of this research: cloud tenants that discover patterns of misconfigurations and vulnerabilities can therefore be more proactive in addressing similar issues in their own environment.

The case studies reported in CSA investigates both the successes and failures in securing cloud environments. By dissecting the reasons and IoC on what contributed to the security failures, CSA also imparts lesson learned and best practices for levelling up an organization's cloud security posture. This knowledge helps organizations wanting to shore up their security regimen and preventing common errors in the cloud environments.

Furthermore, CSA applies cutting edge analytics and visualization technologies to communicate the results in an accessible and prescriptive way. Tools such as Prometheus&Grafana are used to generate intuitive interactive dashboards and reports, which concentrate on the most relevant measures, trends and insights from specific case studies. This visualization improves understanding of intricate security challenges, and facilitates fact-based decisions and actions.

F. Continuous Improvement and Adaptation (CIA)

Continuous Improvement and Adaptation (CIA) – one of the core principles of DCSF – is aimed at making sure the Framework remains effective in the face of changing cloud environments and ever-evolving threats. CIA empowers our community to continuously improve and adapt the CSPM platform through feedback loops used to refine and adapt the platform based on emerging threat landscapes, user feedback and security incidents. This iterative process ensures that the security posture remains robust and proactive to new challenges.CIA in cloud environments collects and checks security pathways to be reformed. CIA also collects a certain variables including security audits, threat information feeds, and incidents to point out problems and possible pathways for improvement.

Furthermore, CIA receives input and collaboration from users to augment the success of the DCSF. By involving users and gathering their input, organizations can ensure the CSPM platform reflects their environment’s unique problems and questions. This approach enhances a

culture of continuous improvement and encourages the sharing of best practices and lessons learned. In order to facilitate the process of continuous improvement, DCSF integrates with next-generation analytics and machine learning platforms like ELK Stack, to provide strong distributed data processing and analysis capabilities, helping organizations get actionable insights from tremendous amount of security data. By using these tools, CIA can identify emerging threats as they begin to surface, predict potential security incidents, and launch proactive measures which could help reduce the risk of possible loss.
Additionally, CIA makes sure to outline the caliber of education and initiative that security teams should have. CIA states that security teams should have continuous training a certification from the providers of the Cloud Security Alliance. Ongoing, updated training will keep the security team up to speed on the latest and greatest in what threats are happening in real time, and how to defend against them.

IV. EXPERIMENTAL SETUP AND RESULT ANALYSIS

The successful deployment of the DCSF necessitates an extensive and thorough experimentation environment that can provide evidence of its efficiency within real-world cloud infrastructures. Figure 2 shows the experimental setup used for DCSF proof-of-concept (PoC). The experimentation environment has five steps. First, ManageEngine is interconnected to begin the Automated Configuration Audits (ACA) procedure. ManageEngine is spreaded throughout three major cloud service providers including, AWS, Azure, and Google Cloud. After this, ManageEngine is properly configured for continuous compliance checks. By evaluating the existing configurations, security baselines are created and any deviations or misconfigurations are recognized. Third, the automated configuration audits are executed and troubleshooting reports are formulated, demonstrating compliance and recommending solutions to manage accordant faults in the system.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

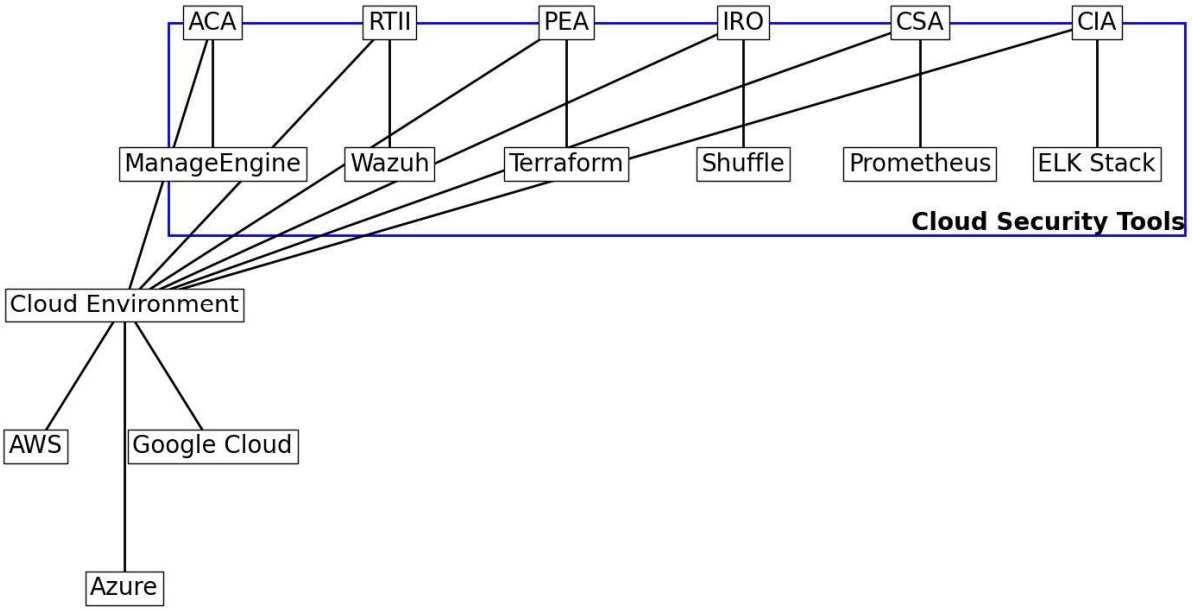

Figure.2 Experimental Setup

To validate the accuracy of DCSF in incident detection and response, the remediation actions suggested by ACA are implemented through simulated configuration changes appearing as an adversary attempt. We also confirm that any form of adversary's credential leaks, suspicious access identities, and internal privilege escalations are surely detected by ManageEngine DLP solutions. All the attacks are conducted through CloudRange, a well-defined adversary model carefully designed for cloud security prototypes. Finally, any successful attacks, the meaningfulness of discovered weaknesses, and the consequence of employed response measures are analyzed.

To enhance Real-Time Threat Intelligence Integration (RTII), Wazuh is deployed in combination with the integration of ThreatConnect, Anomali, and IBM X-Force. EXTRACTOR receives indicators of compromise (IOCs) and sends them to Wazuh for processing. In every cloud instance, we install Wazuh agents to have full event logging/monitoring coverage. The threat intelligence feeds offered by ThreatConnect, Anomali, and IBM X-Force are integrated directly in Wazuh. Therefore, we have their continuous updates available in every platform and we can check what is going on in the different threat landscapes. With IOCs from the feeds, EXTRACTOR will process them and will extract data such as IP addresses, domain names, file hashes, etc. associated with malicious activities. Processing IOCs and after have them associated with a system event/failure was one the most wished features requested from Wazuh users. We have a great product and it is built in a way that we have multiple logs/event about the same thing , so it gives a good correlation for us to find the malicious activities in the logs/events. We evaluate our system with multiple different TTPs (Tactics, Techniques, Procedures) to see the effectiveness of the system detecting the IOCs from real/known threats.

The ability to apply Policy Enforcement Automation (PEA) within the DCSF is accomplished using Terraform, an infrastructure-as-code technology. Terraform scripts are written to encapsulate security policies, including access control rules, encryption obligations, and network security configurations. These scripts are maintained alongside other versions in a version-controlled repository and deployed through CI/CD pipelines to ensure a uniform outcome is achieved across every cloud asset. We verified the usefulness of the PEA component by performing specific use cases where our cloud resources have been deliberately misconfigured. We evaluated the Terraform's competence to discover these misconfigurations and to automatically fix them. The emphasis of our investigation will be both the speed and degree of policy enforcement logic.

To enable the Incident Response Orchestration (IRO) Shuffle integrates with ManageEngine UEBA (User and Entity Behavior Analytics) along with the SOAR platform such as Splunk Phantom, or Palo Alto Networks Cortex XSOAR. Shuffle is configured to orchestrate the incident response workflows by including ManageEngine UEBA for behavior analytics and also including the SOAR platform to automate the response actions. The IRO components are tested with credential theft, data exfiltration, DoS attacks. Shuffle challenged the system with these attacks and also evaluated the response time and accuracy of detecting, analyzing, and mitigating these attacks. The predefined playbook helps to standardize the process of incident response. The predefined playbook ensures every security response follows the same procedure. Also, Shuffle integrates the communication tools such as Slack or Microsoft Teams that can ensure better communication during the incidents.

The process of Case Study Analysis (CSA) leverages the deployment of Prometheus and Grafana to create interactive dashboards that display security metrics and trends. Prometheus is responsible for collecting assortments of metrics from both security tools and cloud resources. By using Grafana, the security investigator will have a perfect view about the security posture on the entire cloud environment through graphical dashboards. For experimentation purpose, it will have some detail case studies gathered from real world cloud deployments that cross almost every industry. Those case studies will simulate the security incident by injecting the deployment errors, vulnerabilities to the system repeatedly. The testing results from multiple case studies will show whether DCSF has ability to detect and mitigate those misconfigurations and vulnerabilities. Those information will also give insights to keep the DCSF updating continuously.

Continuous Improvement and Adaptation (CIA) is enabled by the ELK Stack such as Elasticsearch, Logstash, and Kibana that provide advanced analytics and machine learning with a unified view of massive security data collected in the cloud. Machine learning models are developed and trained by using historical data to predict possible incidents and recommend measures to avoid occurring. To gather information and update security policy gap, the feedback loop in place on analyzing data from audits, incident responses and threat intelligence feeds. It’s

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

very important training the security teams in a continuous manner to make sure their personnel are equipped with knowledge and skill set.

Attack Simulation

In order to thoroughly test the DCSF (Distributed Cloud Security Framework), a series of attack simulations are carried out as part of the experiment setting. The attack simulations consist of real-world scenarios that mimic common attack vectors that target cloud environments. These attack scenarios will evaluate the effectiveness of the DCSF's detection, response, and mitigation against these attacks. Theft of credential simulation covers the attack scenario where an attacker compromises a user's credentials to gain an authorized access to the cloud resources. We evaluate the RTII component's ability in detecting unusual login patterns as well as IRO's response actions in place to safeguard the system from unauthorized access.

Data exfiltration simulations involve the unauthorized extraction of sensitive data from a cloud environment. Here, we evaluate the ACA and PEA components. Assess ACA capacity to uncover misconfigured data stores and PEA's enforcement of encryption policies. Our simulations measure the system's ability to stop unauthorized data transfers and affirm the safekeeping of sensitive information. In denial-of-service (DoS) attack simulations, cloud resources are overcome, grinding services to a halt. We assess RTII's detection capabilities and IRO's automated response actions (e.g., traffic throttling, instance scaling) that ensure service availability.

During ransomware attack simulations, cloud data is encrypted and a ransom is demanded in order to test the "backup and recovery configuration" compliance checks in the ACA component as well as the "incident response workflow" in the IRO component. They allow the DCSF to affirm with certainty whether or not it can effectively "detection of ransomware activity that leads to the triggering of appropriate response actions", and whether the restoration of "all" data in the cloud operation can be achieved without paying any ransom whatsoever. Each simulation is carefully planned and executed under controlled conditions so as to avoid unsafety and to reduce the impact on an actual cloud operation to a minimum. The overall success of attack simulations during all scenarios offers a helpful overview of where the framework stands, as well as what can be done further to improve the framework.

V. EXPERIMENTAL EVALUATION

In order to experimentally evaluate the DCSF, a set of attack simulations are performed in order to assess how well the framework performs. The Automated Configuration Audits (ACA) is evaluated based on how well the ManageEngine creates compliance reports and the reports are accurate and complete. The detection of the misconfigurations and the suggestion of the remediation actions that will be needed are critical because without it, their cloud is not well maintained. The ACA's further effective evaluation is done through having periodic audits and simulated configuration changes in order to make sure there is continuous compliance to the best security practices and regulatory standard.

In order to evaluate the Real-Time Threat Intelligence Integration (RTII) component, we assess its ability to accurately correlate threat intelligence with the cloud environment data, and to promptly raise alerts. The integrated solutions with the ThreatConnect, Anomali and IBM X-Force, along with the EXTRACTOR tool to process the IOCs, gives a comprehensive detection capability to the threats. To evaluate the system performance, we use attack simulations to measure the speed and accuracy of detection and response to the threat. Staying updated with recent threat intelligence and pro-activeness to defend emerging threats are essential for being in accordance with the maintenance of cloud security.

The evaluation of Policy Enforcement Automation (PEA) with Terraform centered on assessing the consistency and reliability of security policy enforcement. The tests included intentionally misconfiguring cloud resources to ensure the system was able to detect the misconfigurations and automatically apply the assigned security controls.

As described above many of the tests automated reviews which is one of the key attributes of PEA. Were PEAR to have been manually reviewed there would have been no recourse other than to read all of the code to find the problems.Finally the effectiveness of the PEA component is measured by the speed and accuracy at which it can enforce policy so as to ensure the cloud remains compliant with organizational standards and regulatory requirements.The evaluation of Incident Response Orchestration (IRO) will be based on the system's ability to coordinate and automate incident response workflows using Shuffle, ManageEngine UEBA, and a SOAR platform. The response time and accuracy of the IRO component will be measured by simulating security incidents and evaluating how quickly and efficiently it detects, analyzes, and mitigates those incidents. The integration of communication tools facilitates real-time collaboration during incidents, leading to better decision-making and situational awareness.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

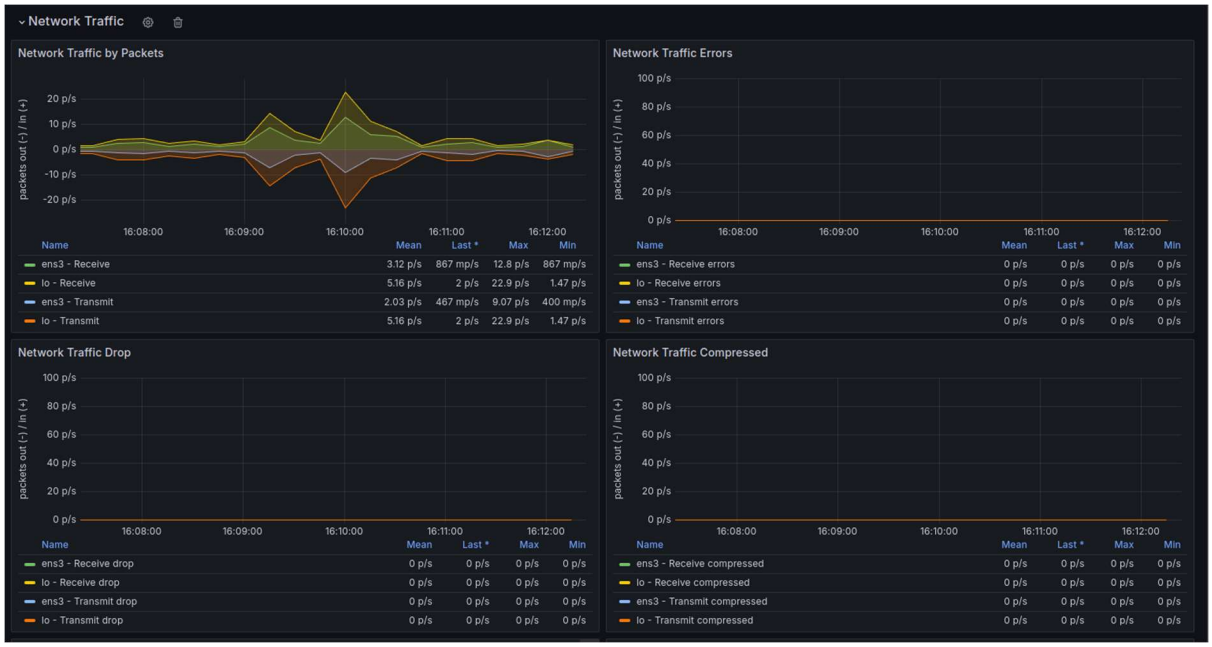

Figure 3. Network Traffic recorded during data exfiltration

A review of the Case Study Analysis (CSA) is carried out using the knowledge gained from in-depth case studies of actual cloud deployments around the world. Security metrics and trends are visualized in dashboards using Prometheus and Grafana, providing an all-encompassing picture of the security condition of the cloud surface. By redoing security incidents observed in different industries, the value of the CSA module is assessed, and the DCSF's sensitivities to prevent and mitigate misconfigurations and exposures are assessed. By trading these inputs, the frame is regularly optimized, resulting in flexible and effective effects.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

Figure 4. System processes during ransomware attack

Continuous Improvement and Adaptation (CIA)'s effectiveness is determined by the system's ability to always monitor, investigate and improve its cloud security posture by using the ELK stack. Machine learning models developed and trained on historical data are evaluated by real-time analysis and decision-making. By having regular feedback loops and continuing training sessions, security team members are provided with the latest knowledge and skills to enhance their overall capability and prepare for emerging and new threats.

Figure 5. Traffic pattern during attack condition.

Figure 3 shows the network traffic patterns detected during data exfiltration attack. Figure 3 also provides a visual representation of data flows within the cloud environment to an external destination during an unauthorized data transfer. It also highlights the key indicators and anomalies associated with such an event. Figure 4 illustrates the behaviour and characteristics of system processes observed during a simulated ransomware attack. Figure 4 provides a visual representation of ransomware affects over system operations, highlighting key indicators and anomalies that are indicative of such an attack. Figure 5 illustrates the network traffic patterns observed during a simulated attack condition. This figure provides a visual representation of how network traffic changes under the stress of a cyber-attack, highlighting key indicators and anomalies associated with malicious activities. Understanding all these patterns is crucial for detecting and mitigating attacks in an enterprise cloud environments.

VI. CONCLUSION

DCSF is a major step forward in cloud security, specifically designed to meet the unique, ever-changing challenges posed by today’s cloud environment. As organizations continue to move more of their business processes and applications to the cloud, the need for a security posture that is as complex and as dynamic as the cloud environment. DCSF delivers a holistic offering inclusive of automated configuration audits, real-time threat intelligence integration, policy enforcement automation, incident response orchestration, continuous improvement and case study analysis full of insight, by integrating ManageEngine, Wazuh, ThreatConnect, Terraform, Shuffle, Prometheus, and ELK Stack; proving it to be a practical and effective solution to enhance cloud security. DCSF also provides a broad and adaptive approach to cloud security, which is critical for securing dynamic cloud environments. The effectiveness of DCSF in different attacking scenarios

demonstrates its ability to mitigate risks and improve incident response capabilities. It enables quick and controlled responses to all security incidents, ensuring that damage is minimized and resilience is promptly restored.In future, in order to sustain with the quickly changing cyber threat landscape, research must concentrate on developing more profound automation for incident recovery, improving the framework's capabilities through more advanced machine learning for predictive threat analysis, and generate a more expansive integration with more cloud service providers.

REFERENCES

[1]. AAbdo, N., Karamany, T. S., & Yakoub, A. (2024). A hybrid approach to secure and compress data streams in cloud computing environment. Journal of King Saud University. Computer and Information Sciences/Mağalaï Ğam'aï Al-malīk Saud : Ùlm Al-ḥasib Wa Al-ma'lumat, 36(3), 101999.

[2]. Alani, M. M. (2024). HoneyTwin: Securing smart cities with machine learning-enabled SDN edge and cloud-based honeypots. Journal of Parallel and Distributed Computing, 188, 104866.

[3]. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials, 17(4), 2347–2376.

[4]. Al-Hawawreh, M., & Hossain, M. S. (2024). Digital twin-driven secured edge-private cloud Industrial Internet of Things (IIoT) framework. Journal of Network and Computer Applications, 103888.

[5]. Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2016). Dual-Server Public-Key encryption with keyword search for secure cloud storage. IEEE Transactions on Information Forensics and Security, 11(4), 789–798.

[6]. Dalabanjan, G., & G, N. D. (2024). Enabling Attribute-based Access Control for OpenStack Cloud Resources through Smart Contracts. Procedia Computer Science, 233, 861–871.

[7]. Duncan, R. (2020). A multi-cloud world requires a multi-cloud security approach. Computer Fraud & Security, 2020(5), 11–12.

[8]. Galego, N. M. C., Martinho, D. S., & Duarte, N. M. (2024). Cloud computing for big data analytics How cloud computing can handle procesing large amounts of data and improve real-time data analytics. Procedia Computer Science, 237, 297–304.

[9]. Gan, Q., Wang, X., Huang, D., Li, J., Wang, C., & Liu, Z. (2024). Online/offline remote data auditing with strong key-exposure resilience for cloud storage. Computer Standards & Interfaces, 88, 103798.

[10]. Gong, Z., Li, J., Lin, Y., Yuan, L., & Gao, W. (2024). A novel dual cloud server privacy-preserving scheme in spatial crowdsourcing. Computers & Security, 138, 103659.

[11]. Graham, R. L. (1969). Bounds on multiprocessing timing anomalies. SIAM Journal on Applied Mathematics, 17(2), 416–429.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

[12]. Guo, J., Tian, C., Lu, X., Zhao, L., & Duan, Z. (2024). Multi-keyword ranked search with access control for multiple data owners in the cloud. Journal of Information Security and Applications, 82, 103742.

[13]. Haddaji, A., Ayed, S., & Fourati, L. C. (2024). A novel and efficient framework for in-vehicle security enforcement. Ad Hoc Networks, 158, 103481.

[14]. Hasimi, L., Zavantis, D., Shakshuki, E., & Yasar, A. (2024). Cloud Computing Security and Deep Learning: An ANN approach. Procedia Computer Science, 231, 40–47.

[15]. Hu, B., Zhang, K., Gong, J., Wei, L., & Ning, J. (2024). Designated server proxy re-encryption with boolean keyword search for E-Health Clouds. Journal of Information Security and Applications, 83, 103783.

[16]. Sibi Chakkaravarthy Sethuraman, Devi Priya, Saraju P Mohanty, “Flow based containerized honeypot approach for network traffic analysis: An empirical study", Computer Science Review, Elsevier, vol. 50, 100600, 2023.

[17]. Jeremiah, S. R., Azzaoui, A. E., Xiong, N. N., & Park, J. H. (2024). A comprehensive survey of digital twins: applications, technologies and security challenges. Journal of Systems Architecture, 151, 103120.

[18]. Kaur, M., & Verma, V. K. (2024). Cooperative-centrality enabled investigations on edge-based trustworthy framework for cloud focused internet of things. Journal of Network and Computer Applications, 226, 103872.

[19]. Devi Priya, Sibi Chakkaravarthy Sethuraman, Muhammad Khurram Khan, “Container Security: Precaution levels, Mitigation Strategies, and Research Perspectives", Computers & Security, Elsevier, vol. 135, 103490, 2023.

[20]. Khan, S., Jiangbin, Z., Irfan, M., Ullah, F., & Khan, S. (2024). An expert system for hybrid edge to cloud computational offloading in heterogeneous MEC-MCC environments. Journal of Network and Computer Applications, 225, 103867.

[21]. Kiatipis, A., & Xanthopoulos, A. (2024). Cloud usage for manufacturing: Challenges and opportunities. Procedia Computer Science, 232, 1412–1419.

[22]. Kumar, K. P., Prathap, B. R., Thiruthuvanathan, M. M., Murthy, H., & Pillai, V. J. (2024). Secure approach to sharing digitized medical data in a cloud environment. Data Science and Management, 7(2), 108–118.

[23]. Sibi Chakkaravarthy Sethuraman, Aditya Mitra, Kuan-Ching Li, Anisha Ghosh, M Gopinath, Nitin Sukhija, "Loki: A Physical Security Key Compatible IoT Based Lock for Protecting Physical Assets", Vol. 10, Pages. 112721-112730, IEEE Access, 2023.

[24]. Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Computer Law and Security Report/Computer Law & Security Report, 52, 105931.

[25]. Lakhan, A., Mohammed, M. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., Nedoma, J., & Martinek, R. (2024). A multi-objectives framework for secure blockchain in

fog-cloud network of vehicle-to-infrastructure applications. Knowledge-based Systems, 111576.

[26]. Liu, C. (2024). HPCLS-BC: A novel blockchain framework using heterogeneous peer-node and cloud-based ledger storage for Internet of Things applications. Future Generation Computer Systems, 150, 364–379.

[27]. Liu, Q., Zhou, F., & Chen, H. (2024). Secure Medical Data on Cloud storage via DNA Homomorphic Encryption technique. Physical Communication, 102295.

[28]. Liu, Z., Jiang, C., & Xu, C. (2024). A portable blind cloud storage scheme against compromised servers. Journal of Systems Architecture, 146, 103037.

[29]. Maiti, S., Misra, S., & Mondal, A. (2024). MBP: Multi-channel broadcast proxy re-encryption for cloud-based IoT devices. Computer Communications, 214, 57–66.