A Zero Trust Approach to Cloud Resource Access Request Management and Authorization

DEVEN NANDAPURKAR[1], DR. SMITA CHOUDHARI[2], ATHARV NALWADE[3], CHINMAY KALE[4], YASHVARDHAN JADHAV[5]

[1,3,4,5]Department of Computer Engineering, Marathwada Mitra Mandal's College of Engineering

[2]Assistant Professor, Department of Computer Science, Marathwada Mitra Mandal's College of Engineering

Abstract— In line with the Zero Trust philosophy, this study presents a complex solution that optimizes AWS IAM access control inside a networked architecture. The cornerstone is the Access Management Module, which uses a Zero Trust perspective to enable easy provisioning, modification, and revocation of user access to AWS services. The Continuous Monitoring Module examines CloudTrail logs in real-time, using anomaly detection algorithms to proactively detect security violations and rigorously compare user records against enterprise limitations. The Usage Reporting Dashboard facilitates informed decision-making by offering visually intuitive analysis that aligns with Zero Trust principles. Following the Zero Trust tenet, the Predictive Modeling Module uses past data to train a machine learning model for dynamic risk assessment, strengthening the system's defenses against potential threats. With the help of this integrated architecture, an effective Zero Trust-oriented AWS IAM Access Management Portal is established, successfully handling changing access control and security concerns.

Index Terms— IAM (Identity Access Management), ZTM (Zero Trust Management), ZTNA (Zero Trust Network Access), AMM (Access Management Module), ABAC (Attribute-Based Access Control), NIST (National Institute of Standards and Technology).

I. INTRODUCTION

Today, with cloud computing becoming more and more popular and technology developing at a rapid pace, it is critical to securely and efficiently control access to cloud resources. The way we handle security needs to change as a result of the way information technology is developing and the way threats are becoming more sophisticated. In order to meet this requirement, the creation and deployment of a Cloud Resource Access Request Management and Authorization platform are at the forefront, with the aim of creating a strong system that maintains the highest levels of security and accountability while simultaneously facilitating access to cloud resources.

Historical cyberattacks, such the Stuxnet virus that targeted SCADA systems and cyberattacks on vital infrastructure, give this mission more urgency. Because they are focused on perimeter-based designs, traditional security models find it difficult to adjust to the constantly changing landscape of modern technology. A more advanced and flexible security strategy is required in light of the emergence of cloud computing, the Internet of Things (IoT), and the growing popularity of telecommuting—especially in light of the COVID-19 epidemic. Our project uses a Zero Trust Approach to Cloud Resource Access Request Management and Authorization in response to these difficulties. Our platform, which is in line with the NIST Zero Trust Architecture, aims to rethink the procedures involved in requesting, approving, and managing access to cloud resources. At its core, Zero Trust treats all entities, including users and devices, as untrusted by default, severing trust from an object's physical position within the network. This calls for strict identification verification and ongoing trust assessment. This R&D project carefully investigates how to create a platform that combines cutting-edge security features with a streamlined process for requesting access to cloud resources. Our platform allows users to request access in a standardized and professional manner. It also makes sure that every request goes through rigorous authentication and authorization procedures, which helps to avoid resource misuse and improves the overall security posture of cloud-based infrastructures.

II. PROBLEM DEFINITION

Our initiative tackles important cloud resource management issues. Because of their inherent drawbacks, traditional security methods find it difficult to stay up with contemporary cyberthreats. The risk of illegal access and possible resource misuse is increased by the absence of standardization in the current processes for requesting and managing access to cloud resources. Furthermore, these models have trouble adjusting to the ever-changing environments of telecommuting, cloud computing, and the Internet of Things (IoT). The issue at hand is how ineffective the security models in use today are at providing reliable access control in the rapidly changing environments of telecommuting, cloud computing, and the Internet of Things. The risk of resource misuse and illegal access is increased by the absence of uniformity. Modern cyber threats are dynamic, and traditional security measures are not able to keep up. This calls for a more sophisticated and efficient approach to cloud resource management. Our project aims to create a simplified platform that incorporates cutting-edge security features and improves access request security. Our platform seeks to develop a more secure, responsible, and effective approach to cloud resource access management by welcoming a Zero Trust Architecture inspired by NIST and emphasizing professional standardization in the access request process. The objective is to rectify the current deficiencies and offer a comprehensive solution that aligns with the changing terrain of cloud security issues.

III. OBJECTIVES OF THE PROJECT

- Develop a User-Friendly Platform for Cloud Resource Access Request Management and Authorization.
- Implement a Zero Trust Architecture inspired by NIST's architecture to decouple trust from physical location, emphasizing identity authentication and continuous trust evaluation.
- Facilitate a standardized and professional approach to access requests, enhancing accountability and reducing the risk of unauthorized resource usage.
- Address cloud security concerns by integrating advanced security measures into the access request and authorization process.
- Provide a comprehensive solution to the evolving challenges of cloud resource management in contemporary technological landscapes.
- Through this initiative, we aim to contribute to the advancement of secure cloud resource access management, aligning with the dynamic needs of modern technology environments. The subsequent sections of this paper will delve into the specifics of our platform's architecture, identity authentication methods, access control mechanisms, and trust evaluation algorithms, highlighting their role in ensuring a secure, accountable, and efficient cloud resource access management process.

IV. PROPOSED SYSTEM ARCHITECTURE

By strategically aligning with the Zero Trust Architecture, the proposed solution comprises an advanced and intricately interwoven architecture intended to maximize AWS IAM access management. Fundamentally, the Access Management Module is a cornerstone that makes it easier for administrators to grant, modify, and revoke user access to AWS resources. Through the lens of Zero Trust, this module embodies the least privilege concept by carefully defining and enforcing fine-grained permissions in strict compliance with organizational security policy. At the same time, the Continuous Monitoring Module keeps an eye on user activity by closely examining CloudTrail logs in real-time. Sophisticated anomaly detection algorithms that are in line with Zero Trust principles proactively discover and alert users to possible security breaches. By methodically comparing user logs to predetermined company limitations, the module strengthens security even further and reinforces the Zero Trust paradigm by quickly identifying and notifying deviations that may be signs of illegal or questionable activity. The Usage Reporting Dashboard is a crucial element that complements the Zero Trust framework. It offers administrators a user-friendly interface that makes it easy to analyze user behavior and resource usage visually. This feature facilitates informed decision-making and supports strategic resource optimization activities in a Zero Trust environment by providing decision-makers with detailed information. By using historical data to train a machine learning model, the Predictive Modeling Module adds predictive intelligence to the system while upholding the Zero Trust principle. In accordance with the continuous verification principles of Zero Trust, this model calculates dynamic risk scores for every user, taking into account risk indicators including device kinds, geolocation, and access times. When a user's risk score exceeds predetermined thresholds, the module uses a threshold-based technique to swiftly activate alarms, strengthening the system with proactive threat mitigation capabilities inherent in the Zero Trust design. These many modules are expertly combined by this integrated architecture to create a reliable and perceptive AWS IAM Access Management Portal that is focused on zero trust. Through the integration of access provisioning, usage reporting, continuous monitoring, and predictive risk assessment in a synergistic manner inside the Zero Trust framework, the system provides a comprehensive solution that skillfully tackles the always changing issues surrounding access control and security in AWS environments.

V. ML MODEL

The Predictive Modeling Module represents a pivotal component within the overarching system architecture, leveraging advanced machine learning techniques, specifically Support Vector Machines (SVM), to classify user access requests and contribute to the computation of a comprehensive risk score. This module operates on a rich dataset curated from historical data, encompassing a diverse array of features such as user attributes, temporal dynamics, and resource-related details. Prior to SVM training, feature engineering is employed to extract relevant information, and rigorous data preprocessing steps ensure the dataset's compatibility and consistency. The SVM model, chosen for its efficacy in binary classification tasks, undergoes a meticulous training process to discern patterns associated with accepted and rejected access requests. Hyperparameter tuning further refines the model, optimizing its performance through careful adjustment of parameters such as the kernel type, regularization parameter (C), and kernel-specific parameters. The evaluation metrics applied to the SVM's performance include precision, recall, F1-score, and area under the Receiver Operating Characteristic (ROC) curve, guaranteeing a robust assessment of its classification capabilities. The output of the SVM model, representing predictions regarding the riskiness of access requests, is seamlessly integrated into the broader risk score computation. This integration harmonizes SVM predictions with other crucial risk factors, notably findings from cloudTrail log analysis. By considering multiple dimensions of user behavior, the system ensures a nuanced understanding of potential security threats. The resulting risk score, a composite of SVM predictions and additional risk pointers, becomes a pivotal parameter in the system's risk assessment framework. Moreover, the risk score plays a pivotal role in the system's alerting mechanism. When the computed risk score surpasses predefined thresholds, alerts are triggered, signaling potential security risks and ensuring timely notifications for administrators. This dynamic and multifaceted approach enables the system to proactively identify and mitigate security threats within AWS environments, offering administrators a comprehensive toolset for effective access management and threat response. In essence, the integration of SVM-based classification with broader risk assessment parameters enhances the system's capacity to discern and respond to evolving security challenges in cloud computing environments. The SVM model was trained to predict the count of rejected requests for users based on historical data, with features including the type of requests (read, write, admin). The model achieved an overall accuracy of 40%. However, it's essential to interpret these results carefully due to the imbalanced nature of the data. The confusion matrix indicates that the model struggled to correctly classify users with 0 and 1 rejected requests, often predicting a count of 2. This is reflected in the classification report, which shows low precision and recall for counts of 0 and 1. On the other hand, the model performed relatively well in predicting users with 2 rejected requests, achieving a precision of 40%, recall of 100%, and an F1-score of 57%. Despite the low overall accuracy, these results suggest that the model might be more effective in identifying users with a higher count of rejected requests. Further optimization and consideration of potential imbalances in the dataset could improve the model's performance.

VI. DESIGN AND ARCHITECTURE

The proposed system architecture centers around efficiently managing user requests for accessing application operations, incorporating multiple decision points and parameters to ensure robust security. The process begins with the "User Request" as the initiator, prompting the collection of "Request Parameters". These parameters serve as essential input for the subsequent stages of the architecture.

The "Access Context Manager" plays a pivotal role in coordinating and contextualizing the request parameters. It serves as a central hub where information such as user identity, access history, and contextual data are gathered and processed. This contextualization lays the foundation for informed decision making throughout the architecture.

The architecture then bifurcates into multiple decision points, each contributing to the final determination of whether the user request is granted or denied. "Admin Approval" is a crucial step where the access request undergoes scrutiny by an administrator, ensuring alignment with established security policies and access requirements. Simultaneously, the "IAM Authentication" process verifies the user's identity, adding a layer of authentication to the request.

The "Risk Analysis of User Activities" component introduces an element of proactive security by assessing potential risks associated with the user's historical activities and contextual information. The "Identity Access Review System" complements this by continuously reviewing and auditing user identities and access rights, contributing to the overall security posture.

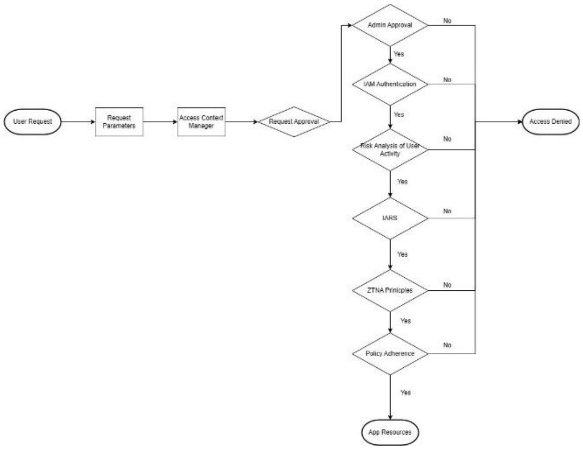

Fig. 1. System Architecture

The incorporation of "Zero Trust Network Access (ZTNA) Principles" enhances security further, adhering to the philosophy of continuous verification and trustworthiness assessment. The system also enforces adherence to predefined policies, ensuring that the access request aligns with organizational guidelines and compliance standards.

The final decision point consolidates these components. If all the preceding decision parameters, including admin approval, IAM authentication, risk analysis, identity access review, adherence to policies, and ZTNA principles, align positively, the user request is allowed to proceed with the desired application operation. On the contrary, if any of these parameters indicate a deviation or non-compliance, the access is promptly denied, safeguarding the application and its resources from potential security threats.

This architecture, by integrating contextual analysis, layered authentication, risk assessment, and adherence to security policies, establishes a comprehensive framework for secure and informed decision-making in granting or denying user access to application operations.

VII. CHALLENGES and FUTURE TRENDS

There are several challenges associated with adopting a Zero Trust Approach to Cloud Resource Access, Request Management, and Authorization for businesses seeking to strengthen their cybersecurity posture. One significant challenge is the complexity of converting traditional access control models to Zero Trust's dynamic and context-aware features. Careful planning and execution are required for this change, along with a thorough understanding of the current systems, user behavior, and resource requirements. Furthermore, there are issues with resource usage and user experience related to the integration of continuous authorization and authentication processes. Businesses must strike a balance between ensuring robust security procedures and facilitating user access to cloud resources. It can be challenging to implement Attribute-Based Access Control (ABAC) effectively, especially in cloud environments with multiple user roles and complex resource dependencies. The potential for increased administrative expenses is a further significant barrier that has to be addressed.

Maintaining policies, user rights, and monitoring tools in a Zero Trust system requires extra administrative labor. Organizations must invest in personnel training and the adoption of efficient technologies in order to speed these processes and lower the likelihood of mistakes or oversights. Moreover, achieving and preserving regulatory compliance in a Zero Trust architecture might be challenging. When updating current compliance frameworks to correspond with the continuous review and risk-based access control of Zero Trust, it is vital to carefully examine and make ongoing adjustments in order to ensure compliance with industry standards and legal requirements. Finally, people accustomed to traditional access control systems could disagree with and mistrust organizations. Successful Zero Trust implementation necessitates addressing user concerns, enlightening users about its advantages, and fostering a security-conscious culture. Overcoming these challenges and achieving a more secure authorization, request management, and cloud resource access framework would require a thorough and deliberate strategy that considers organizational, technological, and human elements.

Future developments could see a number of ways to increase the suggested system’s functionality for people with visual impairments. In order to serve a more varied user base worldwide, the system can firstly profit from expanding its multilingual capability to include a larger range of languages. Improved natural language processing for a more sophisticated comprehension of complicated material can be included into advanced text-to-speech improvements, going beyond simple recognition and reading. Expanding object recognition capabilities can provide comprehensive support in situations such as buffet settings, particularly with regard to distinguishing between different cuisines and dishes. Enhancing facial recognition algorithms will help identify known people more accurately, which will further customize the user experience. Furthermore, by taking into account differences in note conditions, the system’s currency denomination recognition can be improved for increased accuracy in identifying distinct notes. Prospective avenues for future improvement include expanding the voice command recognition module’s comprehension of a wider variety of commands and including all-encompassing GPS-enabled inside and outdoor navigation aid. The system will continue to evolve as a result of user customization options, integration with other assistive technologies, and continual accessibility advances, keeping it at the forefront of inclusive and efficient support for visually impaired users.

CONCLUSION

In conclusion, the proposed system architecture for a Zero Trust Approach to Cloud Resource Access Request Management and Authorization offers a comprehensive solution to the challenges of managing access to cloud resources in contemporary technological landscapes. By implementing a Zero Trust model, the system decouples trust from physical location and emphasizes identity authentication and continuous trust evaluation. This approach facilitates a standardized and professional approach to access requests, enhancing accountability and reducing the risk of unauthorized resource usage. The proposed system architecture includes an Access Management Module, Continuous Monitoring Module, Usage Reporting Dashboard, and Predictive Modeling Module, which work in unison to provide a secure, accountable, and efficient cloud resource access management process. The system's integration of advanced security measures and machine learning techniques contributes to dynamic risk assessment, strengthening the system's defenses against potential threats and erroneous human behavior. Overall, the proposed solution offers a reliable and perceptive Cloud Access Management Portal that skillfully tackles the ever-changing issues surrounding access control and security in dynamic cloud environments.

REFERENCES

[1] V, Akshay & S, Anish & RM, Alagappan & S, Gnanavel. (2019). BOOKAZOR - an Online Appointment Booking System. 1-6. 10.1109/ViTECoN.2019.8899460.

[2] S. Mehraj and M. T. Banday, “Establishing a Zero Trust Strategy in Cloud Computing Environment,” 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104214.

[3] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, “A Survey on Zero Trust Architecture: Challenges

and Future Trends," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-13, Jun. 15, 2022, doi: 10.1155/2022/6476274.

[4] F. F. Moghaddam, P. Wieder and R. Yahyapour, "Policy Engine as a Service (PEaaS): An Approach to a Reliable Policy Management Framework in Cloud Computing Environments," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 2016, pp. 137-144, doi: 10.1109/FiCloud.2016.27.

[5] F. Li, G. Wu, J. Lu, M. Jin, H. An and J. Lin, "SmartCMP: A Cloud Cost Optimization Governance Practice of Smart Cloud Management Platform," 2022 IEEE 7th International Conference on Smart Cloud (SmartCloud), Shanghai, China, 2022, pp. 171-176, doi: 10.1109/SmartCloud55982.2022.00034.

[6] P. Kokkinos, T. A. Varvarigou, A. Kretsis, P. Soumplis and E. A. Varvarigos, "Cost and Utilization Optimization of Amazon EC2 Instances," 2013 IEEE Sixth International Conference on Cloud Computing, Santa Clara, CA, USA, 2013, pp. 518-525, doi: 10.1109/CLOUD.2013.52.

[7] M. Singh, S. Bhushan and S. Rani, "Investigation of SLA Management in Cloud Computing and Future Directions," 2021 2nd Inter-national Conference on Computational Methods in Science Technology (ICCMST), Mohali, India, 2021, pp. 78-83, doi: 10.1109/ICCMST54943.2021.00027.

[8] P. Sharma and V. Jadhao, "Molecular Dynamics Simulations on Cloud Computing and Machine Learning Platforms," 2021 IEEE 14th International Conference on Cloud Computing (CLOUD), Chicago, IL, USA, 2021, pp. 751-753, doi: 10.1109/CLOUD53861.2021.00101.

[9] A. Wylde, "Zero trust: Never trust, always verify," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-4, doi: 10.1109/CyberSA52016.2021.9478244.