MANAGING SECRETS USING CLOUD

Anuradha Annigeri[1], Akshata M[2], Baswa Prasad[3], Manjappa M[4], Nagraj P[5]
Department of Computer Science and Engineering, Guru Nanak Dev Engg. College, Bidar
Visveswaraya Technological University, Belagavi-590018

Abstract- In this age of digital revolution, cloud services are essential to the effectiveness of organizations. The vital need to secure sensitive data, or "secrets," in cloud environments is addressed by this paper. It addresses important issues like ineffective secret rotation, insider threats, weak encryption, access control problems, and compliance gaps while highlighting the importance of platforms like AWS. The goals include improving security, reducing insider threats, guaranteeing compliance, and putting effective secret rotation in place. This paper offers a useful road map for negotiating the challenges of maintaining secrecy in the ever-changing cloud computing environment. This research addresses the growing worries about the security of sensitive data by exploring the crucial field of secrets management. The difficulties encompass problems like insufficient encryption, susceptibilities to insider attacks, and the crucial requirement for effective rotation of secrets. The paper aims to create a strong framework for managing secrets. This paper provides enterprises with a strategic roadmap to reinforce their security protocols in the ever-changing cloud computing environment.
Keywords: Cloud, cybersecurity, encryption, decryption, secrets.

I. INTRODUCTION

As digital transformation changes the way organizations operate, protecting sensitive information has become a major concern. This report examines the key aspects of managing privacy through cloud computing and cybersecurity, with the goal of addressing the challenges organizations face in protecting sensitive data. Using cloud services and cybersecurity practices is a powerful way to reduce threats and ensure privacy. The primary issues which are to be addressed are:

1. Lock It Up Well

Emphasizes robust encryption and security measures to safeguard sensitive information, mirroring the importance of securing valuables in a physical lock.

2. Keep the Right People In

Focuses on precise access controls, ensuring only authorized individuals have entry, akin to allowing only trusted individuals into a secure space.

3. Watch Out Inside To

Underlines the need for vigilant monitoring within the system, reminiscent of keeping an eye on activities within a secure environment to detect and prevent potential threats.

4. Follow the Rules using Secret Manager

Advocates adherence to established security protocols, likened to following rules in a secure environment, with the use of a Secret Manager to enforce and manage these regulations.

5. Change Locks and Check Guests

Encourages regular updates of security measures, equivalent to changing locks, and thorough scrutiny of new entrants, mirroring the importance of verifying and updating access credentials.

II. OBJECTIVES

1. Develop a Comprehensive Secret Management Framework Tailored to Cloud Environments

In the dynamic landscape of cloud computing, developing a comprehensive secret management framework is crucial. This involves creating a structured and adaptable system that aligns with the unique challenges and opportunities presented by cloud environments. The framework must integrate seamlessly with cloud services, utilizing technologies like AWS Secrets Manager or HashiCorp Vault to securely store and manage sensitive information such as API keys, encryption keys, and passwords. It encompasses policies, processes, and technologies to ensure the confidentiality and integrity of secrets while facilitating their efficient usage within cloud architectures

2. Enhance Security and Confidentiality through Improved Encryption and Access Controls

To fortify digital security, a paramount focus is on enhancing encryption methods and access controls. Improved encryption techniques, including robust algorithms and secure key management, ensure that sensitive data remains confidential both at rest and in transit. Access controls are strengthened through meticulous implementation of the principle of least privilege and role-based access controls (RBAC). This ensures that only authorized individuals and systems have access to specific secrets, reducing the risk of unauthorized exposure and potential breaches.

3. Tackle Insider Threats and Minimize Associated Risks

Recognizing the evolving landscape of cybersecurity threats, addressing insider threats is paramount. The framework incorporates measures to identify and mitigate risks associated with individuals within the organization who may pose a threat. This involves deploying advanced monitoring tools, conducting regular audits, and implementing anomaly detection mechanisms to swiftly detect and respond to suspicious activities. By fostering a culture of security awareness and conducting thorough access reviews, the framework aims to minimize the risks associated with insider threats.

4. Manage Secrets (Passwords) Effectively and Efficiently

Effective and efficient management of secrets, especially passwords, is a core objective. This involves implementing automated processes for password rotation, ensuring that credentials are regularly updated to minimize the risk of unauthorized access. Additionally, the framework promotes the use of secure password storage mechanisms and multifactor authentication to enhance the overall resilience of password management. By streamlining these processes, organizations can significantly reduce the likelihood of security breaches and unauthorized access, contributing to a robust security posture in cloud environments.

III. RELATED WORK

This research analysis underscores the multifaceted nature of the cloud computing landscape, where cybersecurity concerns intersect with the dynamics of platform competition. By examining how security measures influence consumer perceptions and market behavior, the article sheds light on the intricate balance that cloud service providers must maintain. The advocation for a proactive approach to cybersecurity that not only mitigates risks but also serves as a strategic advantage in attracting and retaining customers is shown. Moreover, here it underscores the role of regulatory frameworks and industry standards in shaping the competitive landscape, emphasizing the need for collaboration among stakeholders to ensure a secure and thriving cloud ecosystem. Overall, valuable insights for policymakers, industry practitioners, and researchers seeking to navigate the complex interplay between cybersecurity and platform competition in the cloud domain are offered. [3]

Here in this research, presentation of a significant advancement in text encryption methodologies, particularly through their utilization of AES with 12 rounds and dynamic key selection is shown. The approach addresses the critical need for robust encryption techniques to secure sensitive textual data against evolving cyber threats. By increasing the number of encryption rounds and dynamically selecting keys, the proposed method offers a higher level of cryptographic strength, making it more resistant to potential attacks. The article provides a detailed exposition of the encryption algorithm, offering insights into its implementation and potential performance benefits. Furthermore, the practical implications of their approach, highlighting its applicability in various domains where text-based data security is paramount. Overall, the advancement of encryption techniques, offering a promising avenue for enhancing data security in digital communication and storage systems is presented. [13]

The research addresses the critical need for efficient encryption techniques to safeguard data stored in the cloud against unauthorized access and cyber threats. The proposed method emphasizes time-oriented considerations, leveraging latency-based mechanisms to enhance data security while minimizing processing overhead. By integrating encryption processes with time-sensitive parameters, the aim to optimize encryption

efficiency without compromising security standards is seen. The research not only addresses the critical need for robust data encryption in cloud computing but also contributes valuable insights and strategies for improving data security practices in the evolving landscape of cybersecurity threats. [7]

IV. METHODOLOGY

1. The database admin first provisions a database. It can be a personnel database, a database for a project, or anything which has a set of credentials (Username and Password). The admin also configures those credentials with the permissions required for the application to access the Personnel database.
2. After the database has been provisioned. the database admin creates a secret in AWS Secrets Manager and stores the credentials as a secret and also provides a name to that secret. Then, Secrets Manager encrypts and stores the credentials within the secret as the protected secret text.
3. When the application accesses the database, the application makes an API call to the Secrets Manager to fetch the secret information.
4. After AWS Secrets Manager is called, it retrieves the secret, decrypts the protected secret text, and returns the secret to the client application over a secured channel using TLS protocol.
5. The client application resolves the information which includes credentials, connection string, and any other information from the response, and then uses that information to access the database server.

Fig.1 Methodology

Fig.2 Proposed system

The proposed system can be explained through these points-

1. AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, application credentials, OAuth tokens, API keys, and other secrets throughout their lifecycles. Many AWS services store and use secrets in Secrets Manager. Secrets Manager helps you improve your security posture, because you no longer need hard-coded credentials in application source code.
2. Storing the credentials in Secrets Manager helps avoid possible compromise by anyone who can inspect your application or the components. You replace hard-coded credentials with a runtime call to the Secrets Manager service to retrieve credentials dynamically when you need them. With Secrets Manager, you can configure an automatic rotation schedule for your secrets.
3. This enables you to replace long-term secrets with short-term ones, significantly reducing the risk of compromise. Since the credentials are no longer stored with the

application, rotating credentials no longer requires updating your applications and deploying changes to application clients.

V. RESULTS AND DISCUSSION

In the Sage Maker of AWS services, the codes of AES encryption and decryption code is used to ensure the data security in locks with a power of 256-bit encryption.

Fig.3 AES-256 code instance in SageMaker (Jupyter Lab)

Then an instance of EC-2 machine is created in AWS using Amazon Linux feature and a PuTTY private key (.ppk) file to connect it through PuTTY. Using Public IPv4 DNS, the instance of EC-2 is connected to PuTTY.

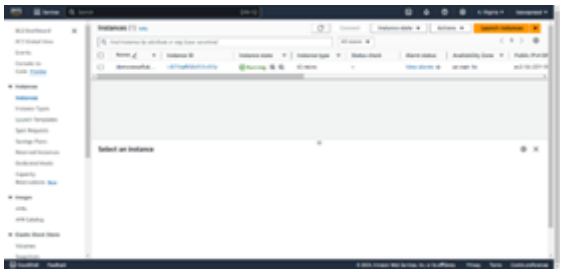

Fig.4 EC-2 machine instance in AWS

Then the public and private key is generated by entering the password.

Fig.5 Generation of public and private key in AWS

The generated public key is added to the SQL worksheet in Snowflake which has the necessary code to connect it through the EC-2 instance.

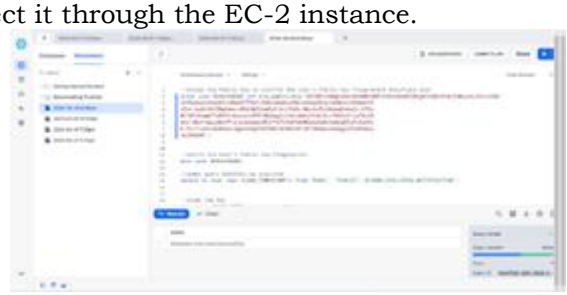

Fig.6 Connecting of Snowflake through generated public key

VI. CONCLUSION

The issues and solutions surrounding the management of secrets in cloud computing environments are covered in detail in this presentation. Organizations can improve security, safeguard sensitive data, and comply with regulations by tackling these problems with a robust privacy management framework. The accomplishment of these objectives depends on

the secure integration of cloud services and data storage systems like Snowflake, AWS RDBMS.

REFERENCES

1. Pedchenko, Yevhenii, YevheniiaIvanchenko, IhorIvanchenko, IrynaLozova, Daniel Jancarczyk, and Pawel Sawicki. "Analysis of modern cloud services to ensure cybersecurity." Procedia Computer Science 207 (2022): 110-117.
2. Pang, Min-Seok, and Hüseyin Tanriverdi. "Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of US federal government." The journal of strategic information systems 31, no. 1 (2022): 101707.
3. Arce, Daniel G. "Cybersecurity and platform competition in the cloud." Computers & Security 93 (2020): 101774.
4. Gupta, Lav, Tara Salman, Ali Ghubaish, DevrimUnal, Abdulla Khalid Al-Ali, and Raj Jain. "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach." Applied Soft Computing 118 (2022): 108439.
5. Zhao, Tiange, Tiago Gasiba, Ulrike Lechner, and Maria Pinto-Albuquerque. "Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings." Journal of Systems and Software 210 (2024): 111946.
6. Rabai, Latifa Ben Arfa, MounaJouini, Anis Ben Aissa, and Ali Mili. "A cybersecurity model in cloud computing environments." Journal of King Saud University-Computer and Information Sciences 25, no. 1 (2013): 63-75.
7. Ahmad, Shahnawaz, and Shabana Mehfuz. "Efficient time-oriented latency-based secure data encryption for cloud storage." Cyber Security and Applications 2 (2024): 100027.
8. Alloghani, Mohamed, Mohammed M. Alani, Dhiya Al-Jumeily, Thar Baker, Jamila Mustafina, Abir Hussain, and Ahmed J. Aljaaf. "A systematic review on the status and progress of homomorphic encryption technologies." Journal of Information Security and Applications 48 (2019): 102362.
9. Moore, Tyler. "The economics of cybersecurity: Principles and policy options." International Journal of Critical Infrastructure Protection 3, no. 3-4 (2010): 103-117.
10. Zineddine, Abdelhadi, Oumaima Chakir, Yassine Sadqi, Yassine Maleh, Gurjot Singh Gaba, Andrei Gurtov, and Kapal Dev. "A systematic review of cybersecurity assessment methods for HTTPS." Computers and Electrical Engineering 115 (2024): 109137.
11. Kundi, D-S., Arshad Aziz, and NassarIkram. "A high performance ST-Box based unified AES encryption/decryption architecture on FPGA." Microprocessors and Microsystems 41 (2016): 37-46.
12. Wadi, Salim M., and Nasharuddin Zainal. "Rapid encryption method based on AES algorithm for grey scale HD image encryption." Procedia Technology 11 (2013): 51-56.
13. Mathur, Nishtha, and Rajesh Bansode. "AES based text encryption using 12 rounds with dynamic key selection." Procedia computer science 79 (2016): 1036-1043.
14. Heron, Simon. "Advanced encryption standard (AES)." Network Security 2009, no. 12 (2009): 8-12.
15. Phan, Raphael C-W. "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)." Information processing letters 91, no. 1 (2004): 33-38.