International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Protecting Data in Amazon S3 Cloud Storage

[1]Ms. Divya Natarajan,[2]Dr. S. R. Raja Associate Professor

[1]Department of Computer Applications Centre for Open and Digital EducationHindustan Institute of Technology and Science Hindustan Deemed University Chennai divya.272206@gmail.com

[2] Department of Computer Applications Centre for Open and Digital Education Hindustan Institute of Technology and Science Hindustan Deemed University Chennai rajasr@hindustanuniv.ac.in

ABSTRACT :

Cloud computing has changed the way the world works. From computing to storage, everything in between and beyond is being developed for the cloud. With corporates, enterprises and governments moving towards cloud and leveraging its benefits, it also raises questions about the security of data being stored and processed in the cloud. Due to the nature and architecture of the cloud security is the most sensitive and often the only factor which dictates the weather an organization will move towards the cloud. In this study, the aim is to address the traditional vs cloud-based scenarios particularly for AWS since it is the pioneer of the cloud revolution. The proposed method is making better use of the cloud and its strengths for storing and securing data automatically.

Keywords: AWS S3, Cloud, Cloud Storage, Data Security, Encryption, Cloud Security

INTRODUCTION :

Cloud Computing Technology is well established and rapidly growing. It has its presence in each technology sector because of the advantages it offers in contrast to the traditional model of computing. While Cloud computing is efficient, affordable, and reliable it does come with a vast list of newfound problems that have originated because of this model. Out of the Many challenges, one of the most concerning factors affecting the Cloud Computing model is Security.

Security at every stage in the cloud is challenged by internal and external factors that may directly or indirectly affect the user of the cloud. Ranging from access to the system, the ill effects of a multi-tenant system, the data at rest in the cloud, the data in transit, the data processed inside the cloud. Unlike physical devices that can be bought to store data, we cannot just store data and forget about it since it is not physically present with us.

The data once uploaded to the cloud may logically be at our reach with the correct access permissions and credentials, but the physical location of the data is well beyond our knowledge which may result in it being stolen, modified, or erased by a malicious entity.

Data that is encrypted is always safer than unencrypted data even if stored in an extremely secured environment. This research aims to provide ways/techniques that can help in achieving data security in the cloud in the most efficient, reliable, robust, and affordable way possible. The study aims to focus on a high-level view of a specific cloud provider, namely - AWS to highlight ways in which the Data security through encryption can be achieved through this cloud service provider's services.

LITERATURE STUDY :

Chenkang Wu, Yonghua Zhu, Shunhong Pan, presents an SLA (Service Level Agreement) evaluation model tailored for cloud computing environments. It explores the dynamic nature of cloud services and how SLAs can be quantitatively assessed. Key contributions include: Importance of SLA in Cloud Services: As SLAs govern cloud provider-user interactions, the authors propose models for ensuring reliability and performance. Evaluation Metrics: It likely introduces quantifiable metrics for SLA compliance. This work contributes to the field by emphasizing quality assurance in cloud services.

S. Mohammed et al., A new lightweight data security system for data security in the cloud computing" Published in Measurement: Sensors, this paper addresses data security in cloud computing with a novel lightweight system. Focus Area: The system likely optimizes encryption and decryption processes to enhance efficiency without compromising security. Modern Relevance: As data security concerns grow with cloud adoption, lightweight methods are increasingly relevant. The authors' DOI link provides further details for those seeking robust, resource-efficient solutions in cloud security.

R. Khande et al, introduces a password security mechanism using AES-256 encryption coupled with PBKDF2 for key strengthening. Methodology: AES-256 ensures strong data encryption, and PBKDF2 adds resistance against brute-force attacks by incorporating salting and key derivation. Practical Application: This mechanism addresses password vulnerabilities by offering a robust framework for securing user credentials. It holds practical implications for secure password management systems.

Hiram Ponce et al, Published in Simulation Modelling Practice and Theory, this research focuses on designing a bio-inspired robot mimicking chameleon locomotion. Key Contributions: Offers insights into bio-mechanics simulation and how natural movements can be emulated. Advances robotics by exploring efficient walking mechanisms through modeling. Impact: It bridges biological inspiration with engineering innovation for potential applications in robotics and mobility. The DOI link provides access to this cutting-edge simulation research.

PROPOSED SYSTEM AND METHODOLOGY :

The Solution to the underlying issues and difficulties faced in mitigating those difficulties is to make use of existing AWS services. These Services are mostly compliant and have their own documentation available on a public forum so that auditors, consultants, and developers while implementing these solutions can view and review the compliance status of individual services. The AWS whitepapers act as a suitable place to start with for the auditors to check each of the services used/mentioned in this study.

The Cloud Service provided by AWS which can help in architecting an encrypted environment for cloud storage is the AWS Cloud Formations. AWS CloudFormation is a service provided by Amazon Web Services that allows users to model and manage technology and security related resources. The template below provides a structure in which data can be encrypted as it comes to the server side of the cloud. The Data when sent through the network to the cloud storage of AWS which is S3, it will be encrypted by using the AWS KMS encryption.

The AWS KMS service helps in encryption and decryption while maintaining cryptographic keys across AWS services in the same account. We aim to prove an AWS KMS key with an encrypted S3 bucket using that KMS key. We encrypt the data object when it is sent to the data storage and decrypts the data when requested by the client. We propose to use the AES-256 to encrypt the data as it is one of the strongest block ciphers available.

The Stepwise Instructions help in understanding the flow and workings of the procedure. The parts consisting of actual encryption can be changed and replaced with the users' own methods of encryption if need be. These steps provide a high-level view of the entire process proposed. It consists of making use of various AWS services and encryption algorithms for Data Upload

The Data to be stored in the cloud is prepared. This step can include organizing the files into folders and archiving them as data is stored in object form. Data is sent to the S3 storage service which is configured by the cloud formation template. Connection to the cloud can be further secured by adding additional steps for adding security in transit. After data is received, the S3 bucket leverages the AWS KMS.

Service for producing a key for the data. By default, AWS KMS uses the AES-256 block cipher which is considered sufficiently secure and robust. The data will be encrypted in an asynchronous way, the keys will be associated with the objects in the bucket and stored in the AWS KMS repository for the account. Data is then sent to the Compute Resource configured for the encryption. In this case we are using the AWS EC2 virtual machines for encryption. The Virtual machine encrypts the objects with help of the KMS service. The Encrypted object is sent back to the S3 cloud Storage and replaced with the data present in the S3 bucket. The new data will be a newer version of the same file since the S3 buckets are version enabled.

The working system flow for Data Download. In this process, when needed the data will send a read request to the S3 bucket with either AWS console, AWS cli or the sdk provided by amazon. The Data object is fetched in the bucket. The key associated with the object is fetched and produced by the AWS KMS service. The Encrypted object is sent to the virtual machine. The keys required for decryption are sent to the virtual machine in this case EC2 instance. The Ec2 instance starts the process of decryption with the acquired key. Decrypted objects are produced as an output and sent to the client device as a response.

IMPLEMENTATION AND RESULTS :

Encryption Process:

API request is sent to KMS to generate Data key using CMK. (You can do that using AWS CLI OR SDK). KMS returns response with Plain Data key and Encrypted format Data key. The actual data (EBS, Local disk data) then can be encrypted using Plain Data key. As the data has been encrypted, you can remove the Plain Data key from the memory. Store Encrypted Data Key somewhere safely. It will be used in future to decrypt the data.

Decryption Process:

Get the encrypted key from your safe. Send an API request to AWS KMS, to decrypt the key. KMS will return response with Plain Data Key. Decrypt the Encrypted Data using Plain Data key.

As the data has been decrypted, you can remove the Plain Data key from the memory.

CONCLUSION :

A model was proposed to be implemented for automated data security using cloud services, encryption, and server-side computation. The method is suitable for individual customers of the cloud and for the parties which opt in for the pay as you go model in the cloud. Generalized security with the proposed solution is not feasible due to SLAs and compliance related issues with the data in question and hence this solution cannot be implemented on the cloud provider's end.

The method discussed provides a way for data to be secured while inside the cloud which otherwise would be unprotected from internal threats of the multi-tenant architecture of the cloud. Data integrity in a shared cloud ecosystem is challenging due to the legal, technological, ethical, and feasibility standpoint. While data encryption being a reliable solution, its implementation becomes challenging due to resources and hardware barriers.

The cloud overcomes almost all these hurdles by using and improving upon the shortcomings of the traditional systems with a slight increase in cost due to computation being done at the cloud servers. This solution leverages the power and features of the cloud to its advantage and unveils a much more efficient way of storing data securely in the cloud.

REFERENCES:

1. Chenkang Wu, Yonghua Zhu, Shunhong Pan, "The SLA Evaluation Model for Cloud Computing", In Proceeding(s) of the International Conference on Computer, Networks and Communication Engineering, pp.331-334, 2013.
2. S. Mohammed, S. Nanthini, N. Bala Krishna, I.V. Srinivas, M. Rajagopal, M. Ashok Kumar, A new lightweight data security system for data security in the cloud computing, Measurement: Sensors (2023), doi: https://doi.org/10.1016/j.measen.2023.100856.
3. Khande, R., Ramaswami, S., Naidu, C., & Patel, N. (2021). AN EFFECTIVE MECHANISM FOR SECURING AND MANAGING PASSWORD USING AES-256 ENCRYPTION & PBKDF2. Technology (IJEET), 12(5), 1-7.
4. Hiram Ponce, Mario Acevedo, Javier GonzálezJuárez, Lourdes Martínez-Villaseñor, Gabriel DíazRamos, Carlos Mayorga-Acosta, Modeling and simulation for designing a line walking chameleonlike legged robot, Simulation Modelling Practice and Theory, Volume 121,2022,102648, ISSN 1569-190X, https://doi.org/10.1016/j.simpat.2022.102648.
5. Cloud Computing Articles, SaaS + PaaS + IaaS. Free Cloud Apps for Educational Institutes: Schools, Colleges, Universities Cloud Computing Services: Appropriate use of online software tools such as Google Apps, Gmail, and Microsoft Live Office by the Michigan State University Community, http://lct.msu.edu/documents/CloudComputingatMSU,guidancedocument,6Sep2011.pdf
6. Amazon Web Services (AWS) Web Site. What is AWS? A comprehensive cloud computing platform. http://aws.amazon.com/what-is-aws/
7. AWS Case Study: Educations.com, Web Site AWS Case Study: http://aws.amazon.com/solutions/cas e-studies/educations-com/
8. Amazon Web Services, Case Study. http://aws.amazon.com/solutions/casestudies/
9. https://aws.amazon.com/whitepapers