International Journal of Computer and Information System (IJCIS)
Peer Reviewed – International Journal
Vol : Vol. 04, Issue 03, September 2023
e-ISSN : 2745-9659
https://ijcis.net/index.php/ijcis/index

Securing a SaaS application on AWS Cloud

1st Siddhartha Sourav Panda, 2nd Nishanth Pathi, 3rdShinu Abhi
M.TECH (Cyber Security), Reva University, Bangalore, Karnataka, India
1st siddharthapanda.cs04@race.reva.edu.in, 2nd nishanthkumar@race.reva.edu.in, 3rdshinuabhi@reva.edu.in

Abstract*—The last few years have seen tremendous growth in cloud adoption especially the new age companies and startups in multiple domains are embracing cloud technologies to avoid on-premises costs of maintaining the systems. As organizations grow and continue to invest in digital transformation, the cloud is becoming an ever more crucial part of the organization. For startups, it is highly required that they look at their cloud security components and make them robust to avoid a cyber-attack and reputation damage. Year after year IT world has been witnessing multiple series of news headlines and data leaks that occurred because of cloud architecture misconfigurations. In this article, the authors will explore Amazon Web Services (AWS), which is one of the top cloud service providers in the world. This paper target is to educate and set up a guideline for a secured architecture baseline on AWS cloud adoption for new or existing customers to review their architecture and encourage them to deploy the security components on AWS. This paper provides a brief overview of the various architectures proposed and implemented that can act as a solution for handling the various issues related to Cloud Computing, especially Cloud Security.

***Keywords*—Cloud Computing, Cloud Security, misconfiguration, Amazon Web Services (AWS), Secured Architecture**

I. INTRODUCTION

Cloud computing is the on-demand delivery of computing power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing. These resources run on server computers that are located in large data centres in different locations around the world. When a user uses a cloud service provider like AWS, that service provider owns the computers that users are using. These resources can be used together to build solutions that help meet business goals and satisfy technology requirements.

Services in the Software as a service (SaaS) category provide a user with a completed product that the service provider runs and manages. In most cases, software as a service refers to end-user applications. With a SaaS offering, users do not have to think about how the service is maintained or how the underlying infrastructure is managed [1]. A cloud-based application is fully deployed in the cloud, and all parts of the application run in the cloud. Applications in the cloud have either been created in the cloud or have been migrated from an existing infrastructure to take advantage of the benefits of cloud computing.

However, problems persist while using cloud-computing services in the IT sector. Many are not sure about its trustability since all the data of companies remain online on the cloud and anyone from anywhere can easily access that data, even leading to data loss [1]. The cloud is comprised of a multitude of settings, policies, assets, and interconnected services and resources, making it a sophisticated environment to fully understand and properly set up. This is especially true for organizations that have been pushed to migrate quickly to the cloud to be in the market also due to the current pandemic situation. Unfortunately, when organizations start using any new technology too quickly without fully understanding its features, misconfigurations could occur.

Research from Vectra indicated that every company surveyed had at least one security issue in its public cloud environment. Client misconfiguration is the fundamental cause of over 99% of cloud breaches [2].

About 90% of Amazon S3 buckets are vulnerable to ransomware attacks due to a combination of high-risk identities and configuration errors, a survey by Ermetic has revealed [3]. Similar are the cases in Elastic Compute Storage which are exposed to the internet on admin ports and data stored as non-encrypted [4]. The databases deployed on the relational database services are most of the time deployed on public subnets and exposed to the internet for ease of admin operations with no data encryption on them [5].

Cloud computing also has other issues like privacy concerns, compliance, security concerns, sustainability, higher costs, and lack of reliability in providing services.

Data at Rest and Data in Transit are two types of data that can pose a security risk in the cloud. The nature of data protection mechanisms, procedures, and processes determines data confidentiality and

integrity. The most important issue is the exposure of data in the two states mentioned. The term "data at rest" refers to data that is stored in the cloud or that may be accessed via the Internet. This includes both backup and production data. The data stored in AWS S3, EBS, and EFS are considered data at rest. The term "data in transit" refers to data that is being moved in and out of the cloud. This data can be in the form of a cloud-based file or database that can be requested for use at a different location. When data is uploaded to the cloud, it is referred to as data in transit at the time of upload. Data in transit is considered riskier than data at rest since it moves across the internet and around enterprise networks. It's also more likely to be exposed to third parties if not handled carefully [6].

II. RESEARCH METHODS

Being a major cloud service provider, AWS provides a highly secured infrastructure and offers a multitude of security services. AWS is one of the top cloud service providers and it provides a variety of managed security services. Moreover, a user doesn't need to worry about maintaining data centres as AWS manages that accordingly. It also provides a bunch of different services like compute, storage, networking, database, etc. to host an application end to end based on user requirements. Users can easily trade capital expenses for variable expenses. Due to these benefits, AWS is trusted by startups, entrepreneurs, and small and medium companies for their architecture hosting. Hosting their infrastructure would save them millions of dollars because with cloud computing they will have the choice to only rent the necessary computing power, storage space, and communication capacity from a large cloud computing provider that has all these assets connected to the Internet. The AWS security services can be integrated with their architecture can be pay-per-use cost. Auto-scaling also equips with guessing the capacity of data. The speed and agility are also increased. Additionally, organizations can easily go global in minutes without spending money or running and maintaining data centres. AWS Cloud Adoption Framework (CAF) provides guidance and best practices to help organizations identify gaps and processes in their architecture. It also helps organizations build a comprehensive and secured approach to cloud computing—both across the organization and throughout the IT lifecycle—to accelerate successful cloud adoption [1].

AWS is a secure cloud platform that offers a broad set of security-oriented products. These services are AWS-managed which means AWS takes responsibility for updating them and patching them to current standards. AWS integrates security in compute, storage, network, database, and other IT resources and recommends exploring these options to improve the security posture.

One main concern of using the cloud is data privacy and security, especially for users with sensitive data that would be destructive to the client if it were stolen. Cloud Computing also attracts the attention of attackers and raises many security concerns as complex architectures get deployed on them. AWS Cloud Security is an emerging sub-domain of network security, computer security, and more vastly information security. It points to a broad set of technologies, policies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Confidentiality, integrity, and availability are three key issues in information assurance. They are also very important in AWS because applications are deployed in a shared network environment. Confidentiality reassures customers that the information being stored offsite on AWS storage can only be accessed by authorized persons. The integrity of the data that is transferred to the AWS cloud is to guarantee that the data has not been corrupted or tampered with during the transit and to keep the data in its original format. Finally, availability is the data and services that are available when it is needed by concerned entities.

Security and Compliance are a shared responsibility between AWS and the customer. This shared model can help relieve the customer's operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws

and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment [7]. AWS is responsible for "Security of the Cloud". AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. The customer is responsible for "Security in the Cloud". Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities [7].

In this paper, the authors will discuss various security challenges and controls in AWS-hosted applications and focus on various AWS-offered services to mitigate the security concerns. By providing such levels of security, the cloud environment could be made more trustable and safer. Security measures and mechanisms could be developed and customized according to the client's organizational needs and must be upgraded frequently to prevent the occurrence of any mishaps.

The literature reviews describe how an unsecured Cloud configuration can lead to cyber-attacks hence causing damage to confidential data leaks and reputation damage. A few authors encourage securing each AWS component and hence the complete architecture remains secured with an overall secured posture.

- Although AWS architecture is designed to be safe, it is up to the users to secure their respective cloud environments. Top data leaks in 2021 demonstrate how simple AWS S3 misconfiguration can lead to sensitive and critical data leaks. A zero-tolerance approach to cloud configurations is the need of the hour. Fixing misconfigurations takes time considering the complexity of the architecture but it should be of the highest priority and organizations must act at the earliest [2]. Multiple AWS services are listed on top AWS misconfiguration lists provided by Trend Micro 2021 report. EBS data storage when non-encrypted and S3 bucket storage when publicly exposed, made into the top 3 misconfigured rules [8].
- Data theft is not the only potential threat. Attackers can also lead to a Ransomware attack encrypting valuable files and demanding compensation illegally. Most S3 buckets are publicly exposed and there are no object scanning mechanisms on the bucket once new files are uploaded which might be malicious [9].
- Databases deployed on AWS RDS can also be vulnerable to attacks when publicly exposed. DB admins open port 3306 open on RDS DB endpoints to connect to the internet and do admin tasks but that opens the attack surface for attackers to take advantage of as well. The DB port should never be exposed on the internet and all data on DB should be stored encrypted with keys [5].
- AWS and multiple security labs recommend configuring proper IAM policies, Bucket policies, MFA, Delete protection, bucket versioning, Data encryption, logging and monitoring, and regular backups for the sensitive and critical data for future action if targeted. So it is highly recommended to audit the bucket configuration frequently to make sure they have secured configuration [10].
- EC2 instances that are supposed to be only privately available should not be exposed to the public internet especially the webserver, software deployment instances, etc. The admin maintenance ports should not be exposed. Security groups and access control lists should be thoroughly reviewed. The data storage disk should remain encrypted with keys and application to be scanned for any potential patches [4].
- AWS provides the best AWS Security features and guidelines on how to use them. It provides best practices for configuration on the AWS cloud. It is a very important pillar in AWS Well-Architected Framework and defines clearly the security foundations and design principles [11].
- The reference web application architecture deployed in this literature reference has been referred for the initial baseline design. Multiple AWS services were deployed on the same to have robust security on the architecture [11].

- According to Cloud Security Alliance, the top 12 cloud security threats have been captured which are faced by organizations on the cloud. They are data leakage, compromised accounts and bypassing authentication, hacking interfaces, and APIs, the vulnerability of the systems used, account theft, insiders, targeted cyberattacks, permanent data loss, lack of awareness, abuse of cloud services, DDoS attacks, joint technologies, common risks [12].
- Misconfigured Amazon S3 buckets can lead to sensitive data leaks and ransomware attacks. When S3 buckets are configured as accessible from the public internet and the objects are accessible then the attacker can get control of the bucket and upload malicious files. Objects can also be downloaded which might contain sensitive data. The bucket policies are sometimes not strict which allows malicious file uploads. DDoS attacks can also be performed on the bucket endpoints exposed to the internet [10].
- If misconfigurations are relatively straightforward to stop, then why are they so common? The cloud is comprised of a multitude of settings, policies, assets, and interconnected services and resources, making it a sophisticated environment to fully understand and properly set up. The organizations are migrating to the cloud without fully understanding each component being integrated and this might cause misconfiguration in a few components [8].
- This research paper explains how big data processing is done using advanced AWS services and how the data can be kept secure on those services. AWS services can secure huge data encrypted and process them efficiently [13].
- Cloud service providers spend a lot of effort and cost to enhance the security of the data flowing through them. This paper analyses the storage encryption and data integrity concepts along with the performance of cloud services [14].
- There are multiple ways the data on the cloud can remain encrypted in secured application architecture. Along with the "data in transit" security it is highly recommended that users look at "data in rest" security. Cloud provides multiple options of either key generating, storing, and encrypting with their native solutions or users can encrypt them with any advanced algorithm before sending them to the cloud. This paper explains how the data can be encrypted at the user end before storing it in the cloud [15].
- Along with secured architecture and data security, it is required to have secure authentication to access cloud resources. In the architectures, the authors have proposed the usage of an Identity Provider service like Cognito which handles users' registration and authentication. Also, for admin-level users, the authors have proposed the usage of bastion hosts with dedicated SSH keys. This paper briefly explains the advanced Kerberos authentication with LDAP role-based access control which can be integrated with cloud computing applications [16].
- This review paper describes various benefits of migrating to the cloud and a few security issues with the cloud as well. As it depends on organization requirements if the advantages of the cloud benefit them, they can plan on migrating to the cloud [17].
- In the proposed architectures the authors have integrated AWS Guard Duty threat intelligence device for alerting and capturing malicious attempts. Guard duty is an advanced service and contains updated and recent security standards rules to recognize malicious attacks. But any service cannot be perfect so it is also desirable if an organization would like to integrate an additional IDS/IPS with the secured architectures [18].

III. RESULTS AND DISCUSSION

This paper proposes two different architectures for hosting a web application or a web server on the AWS cloud. The architectures explain methods of how an organization can migrate their web application to the cloud and how to integrate the services offered by AWS to secure them. The AWS-offered services are updated to current security trends by AWS so an organization can directly utilize them. In this paper, the authors will be explaining the architecture diagrams and the components involved. Organizations can refer to the same for their application hosting on AWS.

The first architecture as in Figure 1 describes a web application deployed on an EC2 instance that is publicly accessible through Application Load Balancer and CloudFront CDN. The instances are spread across availability zones and use auto-scaling. The EC2 webserver interacts with the RDS database for web application users and configuration stored in a database. Users will be connecting to CloudFront URL on TLS connection with DNS hosted by Route 53 and certificate approved in ACM. The web CloudFront is protected by WAF for any web-targeted attacks. Other AWS security components have been integrated with the instance for added security features like Guard Duty, Inspector, etc. All data storage on EBS, EFS, S3, and RDS are all encrypted with keys stored in KMS. Admins can take control of EC2 instances connecting through Bastion Hosts. Based on organization requirements, site-to-site VPN with IPsec tunnel can also be configured for VPN connection from the on-premises data centre to AWS resources.

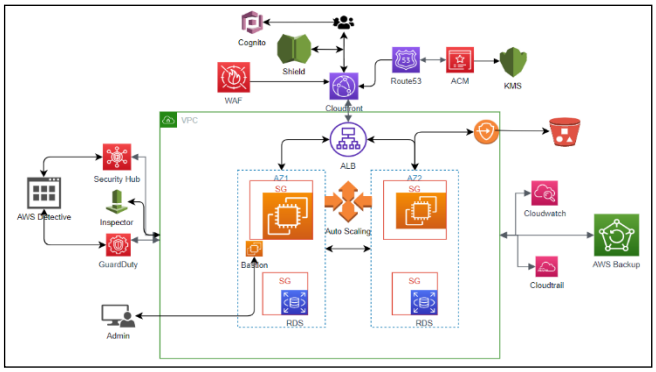

Fig. 1. Web Application Architecture on EC2 Web

server

The following AWS services are integrated into the web application and web server for a robust security posture:

- **EC2 instances**: The web server is deployed on them
- **RDS**: The database service on AWS cloud to store web applications and users.
- **S3**: Bucket service to store the files, objects, etc.
- **Auto Scaling**: The auto-scaling feature is enabled on the instances to make sure the application is not slowing down and performance is not throttled.
- **ALB**: Application Load Balancer is a fully managed layer 7 load balancing service that load balances incoming traffic across multiple targets.
- **CloudFront**: It is a CDN service that speeds up the distribution of web content across multiple regions.
- **CloudWatch**: It is a monitoring and management service that provides data and logs insights for AWS.
- **CloudTrail**: It enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage.
- **Guard Duty**: It is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect AWS accounts, EC2, and data stored on S3.
- **Inspector**: It is an automated security assessment service that helps identify the vulnerabilities and common misconfiguration on instances.
- **Security Hub**: It is a centralized security management service that performs security best practice checks, and aggregates logs from multiple security services.
- **Detective**: It automatically collects log data from multiple AWS resources and uses machine learning, and statistical analysis to build a linked set of data that enables to easily conduct faster and more efficient security investigations.
- **WAF**: It is a web application firewall that helps protect web applications against common web exploits and thus enhances security.
- **Shield**: It is a DDoS protection service that safeguards applications running on AWS.
- **Route 53**: It is a highly available and scalable cloud domain name system service in AWS.
- **ACM**: It handles the process of creating, storing, and renewing public and private SSL/TLS certificates and keys that protect AWS resources and applications
- **KMS**: It is a secure service that uses hardware security modules to protect keys. It can be used to encrypt and decrypt data.
- **Cognito**: It helps in easily adding user sign-up and authentication to web applications.

- **VPC Endpoint**: It enables to privately connect VPC to supported AWS services without routing on the internet and taking advantage of AWS internal infrastructure
- **Bastion**: It is a server that helps admins to provide access to a private network from an external network.
- **Backup**: It is a fully managed backup service that helps to centralize and automate the backup of data across AWS services.

The second architecture as in Figure 2 describes a web application hosted on an S3 bucket and exposed to the public internet with help of CloudFront. The connection from users to CloudFront DNS is secured with TLS and the domain is hosted on AWS Route 53 which takes the certificate signed by Amazon CA. The data on the S3 bucket is stored encrypted with keys stored in KMS. The S3 bucket is integrated with an antivirus solution that scans for every object uploaded and uses SNS to send notifications to admins if an infected file is found. Other AWS Security components have been closely integrated with the architecture for added security posture.

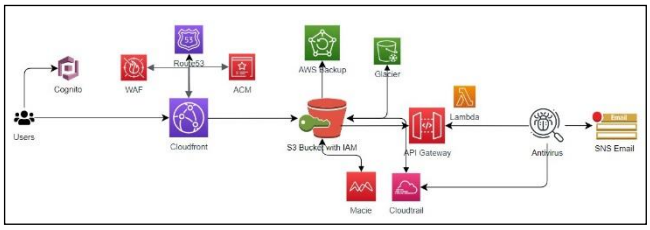

Fig. 2. Web application deployed on S3 bucket

The following AWS services are integrated into the web application and web server for a robust security posture:

- **S3**: Bucket service which stores the web application code objects.
- **CloudFront**: It is a CDN service that speeds up the distribution of web content.
- **CloudTrail**: It enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage
- **Macie**: It is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect sensitive data in S3.
- **API Gateway**: It is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs. It is integrated here with Lambda for an antivirus solution.
- **Lambda**: It is a serverless compute service that runs code in response to events and automatically manages the underlying compute resources automatically. Here lambda function is integrated with S3 Bucket antivirus for object scanning.
- **Bucket Antivirus**: It is a service integrated with S3 buckets and scans any object as soon as uploaded for malware when events are generated for file upload.
- **SNS**: SNS service is enabled to send notifications on email as soon as an infected file is found on the S3 bucket.
- **Route 53**: It is a highly available and scalable cloud domain name system service in AWS.
- **ACM**: It handles the process of creating, storing, and renewing public and private SSL/TLS certificates and keys that protect AWS resources and applications.
- **WAF**: It is a web application firewall that helps protect web applications against common web exploits and thus enhances security.
- **Cognito**: It helps in easily adding user sign-up and authentication to mobile or web applications.
- **Backup**: It is a fully managed backup service that helps to centralize and automate the backup of data across AWS services.
- **Glacier**: It is a low-cost cloud storage service to provide storage for data archiving and backup of cloud data.

IV. CONCLUSION

It is quite evident that multiple architectures on AWS have several risks like data leakage, account hijacking, insecure interfaces and APIs, components misconfiguration, and many more, but by using AWS effectively and understanding each component clearly while deploying secured configuration, users can effortlessly mitigate a lot of these problems. Although there is not a single solution for all issues but from a user perspective, one needs to know the commonly occurring misconfigurations to mitigate them before malicious attackers get to exploit them and cause more significant harm. Lack of awareness of cloud technology and without fully understanding the cloud-

provided services can cause these security misconfigurations and not a secured architecture implementation. With multiple services being developed and released by the cloud it is recommended to understand them as they are developed following current security issues and can control them. The organizations can refer to the proposed architecures on this paper as a baseline for their secured infrastructure deployment or migration to AWS.

As of now, AWS offers over 200 fully featured services from multiple regions globally. These services can be used by following the "pay-as-you-go" model of AWS, by which users only pay for those services they use. In addition to that, AWS offers a variety of other services like scalability, which means AWS balances the size of the server accordingly, and flexibility which indicates that users do not need to worry about processing, data storage, security & integrity. Multiple AWS Secured services are being developed and released and AWS strongly recommends utilizing them to safeguard resources from ever-improving cyber-attacks.

Cloud security should be the highest priority for both organizations and cloud service providers. It includes the ability to protect data, systems, and assets to take advantage of cloud technologies to improve user security. Cloud service providers build security into the core of their cloud infrastructure and offer multiple advanced services to help organizations meet their unique security requirements in the cloud.
In Cybersecurity the main weakness is the human itself and since cloud technologies are advanced and new products and security features are being published in a short period, it is of utmost priority that the user understands the solutions and services before deploying them to production. After all customer data is a treasure and everyone would like to keep their private data safe and secured.

REFERENCES

[1] T. Singh, "The effect of Amazon Web Services (AWS) on Cloud-Computing," *Int. J. Eng. Res. Technol.*, vol. 10, no. 11, pp. 480–482, 2021, [Online]. Available: https://www.ijert.org/research/the-effect-of-amazon-web-services-aws-on-cloud-computing-IJERTV10IS110188.pdf

[2] O. Nath, "Top 5 AWS Misconfigurations That Led to Data Leaks in 2021," 2021. https://www.spiceworks.com/it-security/cyber-risk-management/articles/aws-misconfigurations-2021/

[3] O. Nath, "What Makes AWS Buckets Vulnerable to Ransomware and How to Mitigate the Threat," 2021. https://www.spiceworks.com/it-security/cyber-risk-management/news/aws-vulnerable-to-ransomware-attacks/

[4] A. Mahajan, "4 Most Common Misconfigurations in AWS EC2 Instances," 2021. https://kloudle.com/blog/4-most-common-misconfigurations-in-aws-ec2-instances

[5] Cloudanix, "15 TOP AWS RDS MISCONFIGURATIONS TO AVOID IN 2022," 2021. https://blog.cloudanix.com/top-15-aws-rds-misconfigurations-2022/

[6] N. Lord, "Data Protection: Data In transit vs. Data At Rest," 2019. https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest

[7] AWS, "Shared Responsibility Model." https://aws.amazon.com/compliance/shared-responsibility-model/

[8] Trend, "Top 10 AWS Security Misconfiguration," 2021. https://www.trendmicro.com/en_us/devops/21/k/top-10-aws-security-misconfigurations.html

[9] Votiro, "How Misconfigured Amazon S3 Buckets Can Lead to a Ransomware Attack," 2021. https://securityboulevard.com/2021/04/how-misconfigured-amazon-s3-buckets-can-lead-to-a-ransomware-attack/

[10] S. Gietzen, "S3 Ransomware Part 2: Attack Vector," 2021. https://rhinosecuritylabs.com/aws/s3-ransomware-part-2-prevention-and-defense/

[11] AWS, "Security Pillar AWS Well-Architected Framework," 2020.

[12] S. Malik, "Top 12 cloud security threats according to Cloud Security Alliance," 2021. https://bitbytes.io/cloud-security-threats/

[13] G. K. Anand Mishra, "Big Data Analytics Options on AWS," *Int. J. Eng. Res. Technol.*, vol. 10, no. April, p. 29, 2021.

[14] P. NIKHIL N and M. RAHUL B, "A Comprehensive Survey on Data Integrity Proving Schemes in Cloud Storage," *Ijarcce*, no. December, pp. 8163–8166, 2014, doi: 10.17148/ijarcce.2014.31019.

[15] A. Phapale, "A Novel Approach for Securing Cloud Data Using Cryptographic Approach," pp. 296–299.

[16] N. I. Eltayb and O. A. Rayis, "Cloud Computing Security Framework Privacy Security," ... *Recent Innov. Trends Comput. ...*, no. February, 2018, [Online]. Available: http://www.academia.edu/download/56698026/1519625123_26-02-2018.pdf

[17] M. N. Ujloomwale and M. R. Badre, "Data storage security in Cloud," *IOSR J. Comput. Eng.*, vol. 16, no. 6, pp. 50–56, 2014, doi: 10.9790/0661-16635056.

[18] G. Thomas and P. Janardhanan, "Intrusion Tolerance: Enhancement of Safety in Cloud Computing," *Ijarcce.Com*, vol. 1, no. 4, pp. 238–242, 2012, [Online]. Available: http://ijarcce.com/upload/june/8-Intrusion Tolerance Enhancement.pdf

[19] B. V Akash and R. Murugan, "Authenticated Transfer of Files with Storage and Backup within A Cloud Environment," *Int. J. Eng. Res. Technol.*, vol. 11, no. 02, pp. 259–260, 2022.