INTERNET AND WEB SYSTEMS – I
TERM PAPER

TITLE: A Survey on AWS Cloud Computing Security Challenges & Solutions

ABSTRACT:

Mainly, Amazon provides a wide range of IT solutions for businesses to create their private virtual clouds and maintain full control over their infrastructure. Amazon Web Services (AWS) can be used for both business operations and IT projects. While the cloud offers cost savings and efficiency that attract security professionals, it also raises various security and compliance concerns. In response to these concerns, AWS has introduced EC2 instances to enhance security, especially for highly regulated companies. Cloud computing has its drawbacks, but these drawbacks also offer opportunities to explore various cloud computing-related topics.
One major concern is the security and privacy of data stored and processed on cloud service providers' servers. This paper gave an analysis by reviewing several research papers and studies on cloud computing security and privacy, shedding light on the challenges and problems associated with it. Mainly this article aims to improve our understanding of cloud computing security issues and highlight the techniques and solutions employed by the cloud service industry. Ultimately, the paper's objective is to provide insights into the emerging cloud services market and the upcoming challenges, including issues related to networks.

INTRODUCTION:

Amazon Web Services (AWS) offers a robust and dependable cloud computing platform known for its high availability and scalability, empowering users to develop a diverse range of applications. AWS prioritizes the security, integrity, and availability of customer systems and data, emphasizing the importance of maintaining trust and confidence. Through AWS's self-service capabilities, customers can manage internal processes independently while remaining responsive to external requests. AWS provides a suite of online cloud computing services via the internet on Amazon's website, with Amazon S3 and Amazon EC2 being commonly utilized offerings. The service is promoted as a more accessible, economical, and faster alternative to establishing a physical server farm for substantial processing power. Each AWS region comprises multiple Availability Zones, distinct data centers offering AWS services. The segregation of these zones helps prevent the spread of outages, and users can configure certain services to replicate across Availability Zones, minimizing the risk of service disruptions.

SERVICES OF AWS:

The cloud formation feature offered by Amazon Web Services (AWS) simplifies the creation of a cloud environment, allowing users to incorporate templates from services like VPC, EC2, Elastic Beanstalk, and more with just a single click. This streamlines the replication of applications and IT infrastructure through a straightforward process. For managing simultaneous high demand, users can leverage content delivery platforms such as CloudFront for distributing widely consumed digital products like video and music.

CloudWatch is a valuable tool for collecting, evaluating, and analyzing metrics associated with cloud resources, particularly as virtual infrastructures become more intricate. The rise of "NoSQL" systems, designed for large datasets that can horizontally scale without human intervention, has become prominent in recent years. Amazon's Elastic Compute Cloud **(EC2)** serves as the foundation for creating a virtual network, while the Elastic Cache service is ideal for temporarily storing large, transitory datasets in in-memory storage. The below image represents the different services of AWS

Elastic Beanstalk acts as a programming framework to manage various required services seamlessly. Amazon Elastic MapReduce **(EMR)** allows users to analyze and manipulate different datasets stored in Amazon's data storage services. **IAM** (Identity and Access Management) is provided by Amazon to manage user access to services, facilitating control over permissions for various instances.

For those not ready to embrace NoSQL, Amazon RDS provides a familiar SQL query language and tools to build scalable database systems. **Route 53** serves as Amazon's scalable DNS system, simplifying the management of DNS zones and subzones.

SQS, a message queuing system, facilitates communication between separate applications or components. **Amazon S3**, the Simple Storage Service, serves as a secure storage solution, aligning with company security rules for sensitive data. SWF (Simple Workflow Service) is instrumental in breaking down significant tasks in highly distributed systems, allowing users to schedule, manage, and set up tasks relevant to extensive distributed processes[3].

Lastly, the Storage Gateway service from Amazon enables disaster recovery and backup archiving through a combination of a PC, an Internet connection, and a physical device in the infrastructure. Virtual Private Cloud **(VPC)** within Amazon EC2 further empowers users to establish a private network of server instances.

SECURITY MEASURES OF AWS SERVICES:

AWS integrates security measures into its services and offers comprehensive documentation on utilizing the available security tools. Customers are strongly advised to leverage AWS security capabilities and adhere to best practices when establishing an application environment. AWS places paramount importance on safeguarding the privacy, integrity, and availability of customer data, with a commitment to maintaining trust and confidence.

There are some AWS methods for protecting the cloud infrastructure:

1. **Data Privacy:** Ensuring the security of data is crucial for various methodologies. Employing techniques such as encryption and hiding, AWS offers the capability to encrypt both personal and commercial data within the cloud. Additionally, backup and redundancy processes for services are made transparent, enabling clients to secure their data effectively and maintain the operational continuity of their applications.

2. **Physical Security:** Over an extended period, Amazon has conceptualized and constructed extensive data centers. The global infrastructure of AWS is situated within data centers owned and managed by Amazon. Access to the specific locations of Amazon's data centers is restricted to individuals within Amazon with a legitimate business requirement. Multiple physical security measures are in place to deter unauthorized access to the data centers and ensure their protection

3. **Secure services:** Offering secure and dependable services, the AWS cloud is crafted to ensure safety across all levels. It effectively prevents unauthorized access or usage, all while delivering the level of freedom that clients anticipate.

INFRASTRUCTURE SECURITY OF AWS:

The transition of IT infrastructure to Amazon Web Services (AWS) brings about a new paradigm characterized by shared accountability between the involved parties. AWS assumes responsibility for streamlining operations by overseeing and controlling various facets of a service's infrastructure, spanning from the host operating system and virtualization layer to physical security. Simultaneously, users are tasked with upholding and configuring the security group firewall provided by AWS, as well as managing the guest OS system, including necessary updates and security patches. For enhanced security and compliance, technologies such as host-based firewalls, intrusion detection, or encryption can be employed if there are concerns in these areas**.**

BEST SECURITY PRACTICES:

Most of the people's concerns about safety in a multi-tenant environment are widespread. Each layer of the cloud application architecture demands security measures. Notably, the service provider manages physical security, presenting an additional benefit of cloud utilization. Users, in turn, are responsible for ensuring network and application-level security. Here, we are going to have a detailed discussion of securing cloud applications on Amazon Web Services (AWS). The initial step involves implementing basic security using the tools and features outlined above, followed by the incorporation of additional best practices through conventional means.

1. **Protect Transit Data:** For sensitive or critical data, encrypt the server instance using third-party certification authorities like VeriSign or Entrust. Utilize the shared session key, generated from the server's public key, to authenticate the data to the browser, ensuring encryption in both directions. Employ network security protocols, including gateways and network management, to protect data in transit, guarding against virus assaults or intrusions. Instead of relying on reactive security measures, proactively identify at-risk information and take necessary steps to safeguard it. It is imperative for businesses to integrate information security measures into their cybersecurity strategies, involving user notifications and encryption for sensitive data[2]. Establish procedures for categorizing and assessing all data, regardless of its location, and implement policies to ensure proper safeguards are in place during both storage and access of the data.

2. **Protect Data Stored:** To address concerns about the storage of sensitive or confidential data in the cloud, users should encrypt individual files before uploading them. For instance, employing open source or commercial PGP-based tools, data can be encrypted before saving as Amazon S3 objects and decrypted upon download. This approach is often necessary for building HIPAA-Compatible Applications, especially those dealing with Protected Health Information (PHI). The encryption of files on Amazon EC2 varies depending on the operating system in use [4]. Encrypting data, whether in transit or at rest, presents challenges irrespective of the operating system or technology employed. Losing a password can result in permanent data loss. Therefore, thorough research into the key management capabilities of any products under consideration is crucial.

3. **Manage Multiple Users:** Within AWS IAM, individuals have the ability to create multiple Users and manage the permissions for each within their AWS account. Each User is equipped with a distinct set of credentials for logging in when utilizing AWS Services. This eliminates the requirement to share user credentials and streamlines the process of granting or denying access to a user. Adhering to security best practices, such as the principle of least privilege, can be achieved by assigning unique credentials to each user in an AWS account. This approach ensures that users only possess the authority to access the specific AWS Services and resources essential for fulfilling their respective roles.

4. **Protect Credentials of AWS:** Amazon Web Services (AWS) furnishes two distinct types of security credentials: access keys and X.509 certificates. The AWS access key comprises an access key ID and a secret access key. When authenticating a request submitted through the REST or Query APIs, users must utilize their secret access key to compute a signature. Utilizing HTTPS for query transmission safeguards against tampering during transit.

ANALYSIS:

Analyzing Amazon Web Services (AWS) involves a detailed exploration of its extensive range of services, spanning computing, storage, databases, machine learning, and more. Understanding the nuances of each service, along with their practical applications, is essential for users seeking to leverage AWS effectively. Delving into AWS's security measures is critical, encompassing encryption protocols, access controls, identity management, and real-time monitoring tools. Examining the platform's infrastructure security sheds light on how AWS safeguards both physical data centers and virtual environments from various threats. Furthermore, assessing AWS's response mechanisms to potential security breaches provides insights into its overall security resilience. To optimize security, users must delve into AWS's recommended best practices, encompassing configuration guidelines, encryption implementation, access policies,

and effective use of IAM.

DISCUSSION:

AWS offers a diverse array of services, spanning computing, storage, and machine learning, catering to a wide range of business needs. The robust security measures of AWS encompass encryption protocols, access controls, and continuous monitoring, ensuring the protection of user data. AWS's infrastructure security involves stringent measures at both physical and virtual levels, establishing a secure foundation for its services. Best security practices recommended by AWS, including proper configuration, encryption implementation, and effective IAM use, contribute to a comprehensive security framework for users. The interplay of these elements highlights AWS's commitment to providing a secure and reliable cloud computing environment.

CONCLUSION:

In this paper, the authors discussed different AWS services and their security measures , infrastructure security and security best practices. In recent years, cloud computing has witnessed remarkable growth, particularly in the realm of commercial online applications. The on-demand, pay-as-you-go model has revolutionized access to computing capacity, offering a more flexible and cost-effective approach. Acquiring computing power has become remarkably straightforward. Cloud-based applications enable users to easily purchase products online, initiating and terminating virtual images as needed. Among the popular features of these services, sharing and creating virtual images with other users stand out. The ascendancy of cloud computing has facilitated comprehensive research into its various aspects, unveiling five primary characteristics, three service models, and four deployment methods. Examining secure cloud storage is intricate due to data being stored redundantly or across multiple locations within a chain of service providers.

REFERENCES:

1. https://ieeexplore-ieee-org.umasslowell.idm.oclc.org/document/9788254
2. https://ieeexplore.ieee.org/document/4738445
3. https://ieeexplore-ieee-org.umasslowell.idm.oclc.org/document/9491632
4. https://ieeexplore.ieee.org/abstract/document/6574666