Fortifying the Cloud: Unveiling the Next-Generation Security Model of AWS

Vipin Bihari [1], Asutosh Kumar [2], Arif Mohammad Sattar [3], Mritunjay Kr. Ranjan [4]

[1] Research Scholar, [2, 3, 4] Assistant Professor

[1] P.G. Department of Mathematics & Computer Science, Magadh University, Bodh Gaya, Bihar.
[2] P.G. Department of Physics, Gaya College, Gaya, Bihar.
[3] Department of Computer Science & Information Technology, A.M. College, Gaya, Bihar.
[4] School of Computer Sciences and Engineering, Sandip University, Nashik, Maharashtra. India.

Published in IJIRMPS (E-ISSN: 2349-7300), Volume 11, Issue 3 (May-June 2023)

Abstract

Amazon Web Services (AWS) is a renowned provider of cloud computing services and infrastructure for businesses of all kinds. As organizations shift crucial data and apps to the cloud, security becomes paramount. This abstract describes AWS's security model and efforts to secure client data and prevent unauthorized access. The AWS security model protects client assets with many layers. AWS data centers include tight access controls, surveillance systems, and numerous levels of protection. AWS also meets worldwide security requirements and best practices. The shared responsibility approach governs AWS and customer security. AWS secures the infrastructure, while clients secure applications, data, and user access. AWS offers identity and access management, network security, encryption, and threat detection to help businesses meet security requirements. AWS security relies on identity and access management (IAM) to govern user access to AWS resources. IAM lets organizations set fine-grained access controls, implement multi-factor authentication, and link with identity systems, improving security. AWS protects data in transit and at rest with strong network security. Network access control lists (ACLs) and security groups provide clients granular control over inbound and outgoing traffic in Virtual Private Cloud (VPC) environments. AWS data is protected by several encryption solutions, including key management services for secure key storage and access. AWS monitors and logs to detect and mitigate security risks. AWS CloudTrail, Config, and Guard Duty let clients monitor and audit their AWS environments, detect configuration changes, and detect security breaches and criminal behavior. In conclusion, AWS security protects client data and applications. AWS secures cloud installations through physical, network, data, and identity and access management. Organizations must understand their shared obligations and use security services and features to secure their AWS resources.

Keywords: Amazon Web Services, AWS Resources, Virtual Private Cloud, Identity and Access Management, Network

1. Introduction

Security has emerged as an issue of crucial importance for businesses all over the world as a direct result of the widespread adoption of cloud computing. Cloud service providers have developed comprehensive security models in response to the necessity of protecting sensitive data, ensuring users' privacy, and protecting themselves against cyber threats. Amazon Web Services (AWS), a renowned cloud computing platform that offers a comprehensive set of security controls and services, is an example of the type of provider that falls into this category. A customer's ability to build and deploy their own applications and services can be made more secure by utilizing AWS's security architecture [1], which is designed to provide such a foundation. The AWS platform utilizes a paradigm known as "shared responsibility," in which both AWS and the customer are tasked with certain duties in relation to data safety and protection. Customers are responsible for ensuring the safety of their own applications and data while they are working within the AWS environment. This approach to working together assures the security of the infrastructure that is supplied by AWS. This study will investigate Amazon Web Services' (AWS) security model in great detail, looking at the many different components, features, and recommended procedures that AWS makes use of to secure the safety of its cloud computing services. In this section, we are going to look into the several layers of security that are applied by AWS [2]. These security layers include physical security, network security, access management, data encryption, and monitoring. In addition, we will go through how Amazon Web Services (AWS) conforms with the standards and laws that are prevalent within the business. This will assure clients that their data is secure and that all of their compliance needs are addressed.

1.1. A Model of Responsibility that is Shared

An important component of Amazon Web Services' (AWS) security approach is known as the shared responsibility paradigm. In this configuration, AWS is the entity responsible for ensuring the safety of the cloud services' underlying infrastructure, which includes all of the company's hardware, software, networking equipment, and physical locations. This incorporates things like the security of the data Centre, the architecture of the network, and the maintenance of the underlying equipment. Customers, on the other hand, are responsible for safeguarding their own applications, data, and user access when working within an Amazon Web Services environment. This includes putting in place security mechanisms such as identity and access management, encryption, and restrictions at the application level [3]. AWS ensures a collaborative approach to security by explicitly outlining the division of security responsibilities. This approach gives customers more control while still leveraging the safe foundation that AWS provides.

1.2. Safety from the Elements

The first and most important step in securing an infrastructure is to focus on its physical protection. Amazon Web Services has put in place strict safeguards to protect its data canters and infrastructure from any potential physical dangers. The use of restricted access restrictions, monitoring via security cameras around the clock, perimeter fencing, and stringent environmental controls with an emphasis on fire detection and suppression are all included in these procedures [4]. In addition, Amazon Web Services (AWS) data canters are constructed in a variety of locations across the globe to ensure redundancy and disaster recovery capabilities.

1.3. Protection of Computer Networks

A multitude of different layers of network security protections are incorporated into AWS in order to protect client data and prevent unauthorized access. Customers' instances are kept logically distinct from one another thanks to the network architecture of Amazon Web Services (AWS), which is designed to offer isolation and segmentation. In addition, Amazon Web Services (AWS) provides clients with something called Virtual Private Cloud (VPC), which enables users to build the topology of their own virtual networks while retaining full control over IP addresses, subnets, and network gateways [5]. AWS employs firewalls, intrusion detection systems, and distributed denial-of-service (DDoS) protection techniques in order to shield itself from potential dangers originating from the outside world. Customers also have the option of utilizing the AWS online Application Firewall (WAF) to safeguard their online applications against the various frequent web-based assaults and exploits.

1.4. Access Management

It is essential to have efficient access management in place in order to guarantee the safety of cloud settings. Customers have the ability to govern and manage user access to AWS resources thanks to the comprehensive collection of identity and access management tools that are provided by AWS. This includes the utilization of AWS Identity and Access Management (IAM), which gives clients the ability to set complex access controls, manage user credentials, and enable multi-factor authentication for an additional layer of protection [6]. AWS also offers connectivity with third-party identity providers, which enables clients to utilise the user directories and authentication procedures already in place within their organizations. In addition, Amazon Web Services (AWS) offers customers tools for the centralised management and auditing of user access. These tools ensure that customers have complete visibility and control over the access management methods they utilise.

1.5. The Encryption of Data

Encryption of data is a crucial step in the process of protecting sensitive information stored in the cloud. A variety of data encryption methods, both for use while the data is at rest and while it is in transit, are available through AWS. Customers are given the ability to manage encryption keys and regulate access to encrypted data through the AWS Key Management Service, also known as KMS. Customers have the option of using AWS-managed keys or storing their own keys in a safe location within AWS Key Management Service to encrypt their data. In addition, Amazon Web Services (AWS) offers Transport Layer Security (TLS) encryption for data while it is in transit [7]. This protects data that is being sent between AWS services and the apps used by the client. Customers can additionally enable encryption for data transfer by utilising AWS Certificate Manager and AWS CloudFront. This encryption is automatically enforced for many of AWS's services.

1.6. Observation and Observance of Regulations

Continuous monitoring and compliance are crucial components in the process of preserving the safety of a cloud environment. Customers are able to monitor their resources, identify security events, and gain insights into their infrastructure thanks to the wide variety of monitoring and logging services that are offered by AWS [8]. CloudTrail from Amazon Web Services generates complete logs of API calls made from within an AWS account. This makes auditing, compliance, and security analysis much simpler. AWS complies with a variety of industry standards and certifications, such as ISO 270001, SOC 2, and PCI DSS, to assist its customers in meeting compliance requirements. AWS also offers its customers the

tools and resources necessary to fulfil their unique compliance obligations. These tools and resources include attestation of compliance, documentation, and reports on compliance status.

A secure basis for cloud computing is provided by Amazon Web Services' (AWS) security model, which is comprised of a comprehensive collection of controls, features, and best practises for the industry. AWS ensures that both the supplier and the customer play an important part in protecting their respective areas of responsibility by utilising a concept known as shared responsibility. This model was adopted by AWS. AWS provides businesses with a safe and compliant environment in which they can develop and deploy their applications and services. This is made possible by the extensive physical security, network security, access management, data encryption, and monitoring capabilities that are offered. Organisations are able to take use of the benefits of cloud computing while ensuring the confidentiality, integrity, and availability of their data if they leverage the security model of Amazon Web Services (AWS).

2. Scope of the Study

This study thoroughly examines Amazon Web Services (AWS) security. AWS stores and processes massive volumes of sensitive data for organisations worldwide as a prominent cloud service provider. AWS security procedures must be understood and evaluated to ensure data confidentiality, integrity, and availability. This research examines AWS's physical security, network security, data encryption, access controls, and incident response. We can learn how AWS secures its infrastructure and client data by examining these factors [9]. The research will begin by describing AWS's architecture and services. This will assist you comprehend AWS's environment and security issues. AWS's physical security will be examined next. Examining their data centres' geographical spread, facility architecture, environmental controls, and access restrictions. We can evaluate client data protection against physical risks like theft, natural catastrophes, and unauthorised entrance by knowing how AWS secures its data centres. AWS network security will then be examined. This includes analysing network architecture, traffic management, and security measures to prevent network-based assaults such Distributed Denial of Service (DDoS) attacks, infiltration attempts, and data interception. The research will also examine AWS's Virtual Private Cloud (VPC) and its secure network isolation for clients' workloads. Data security will also need research [10]. AWS's encryption techniques will be examined. Encryption methods, key management, and AWS Key Management Service (KMS) integration for customer key management will be studied. The investigation will also examine AWS's data backup and disaster recovery systems. The research will also include access restrictions and identity management. IAM and SAML, AWS's authentication and authorisation systems, will be examined. The research will examine how AWS helps clients manage user access, create role-based access restrictions, and employ multi-factor authentication to prevent identity theft. The investigation will also examine AWS's incident response practises. This includes monitoring, logging, threat identification and analysis, and security incident response and recovery. We can assess AWS's security detection, response, and mitigation by knowing their incident response framework. Finally, AWS compliance and certifications will be examined. The GDPR, HIPAA, and PCI DSS will be examined. AWS's compliance stance shows their dedication to security and data protection. Finally, this paper analyses AWS's security model. We may assess AWS's cloud security by assessing their physical security, network security, data encryption, access restrictions, incident response, and compliance procedures. This report will assist organisations contemplating or using AWS secure their data and resources.

3. Literature Review

When it comes to protecting the availability, confidentiality, and integrity of cloud-based resources, Amazon Web Services' (AWS) security model is one of the most important factors to consider [11]. The purpose of this literature study is to investigate and evaluate the previously conducted research and professional publications that are relevant to the AWS security model. By going through these sources, we will be able to acquire a full understanding of the various security mechanisms that AWS has put into place and evaluate how effective they are at reducing the likelihood of potential hazards and threats.

The AWS Security Architecture: The AWS Security Architecture was developed to provide a secure basis for cloud-based applications and services. Virtual private clouds (VPCs), security groups, and identity and access management (IAM) roles are some of the important characteristics that are highlighted in an investigation of the architectural components of Amazon Web Services (AWS) security that was conducted by [10]. According to the findings of the research, it is essential to correctly configure these components in order to set up strong security boundaries.

Identity and Access control (IAM): IAM is an essential part of AWS security since it enables the control of user rights and access. As per [12] focuses on Identity and Access Management (IAM) in Amazon Web Services (AWS), and it discusses the roles of identity federation, multi-factor authentication (MFA), and fine-grained access controls. The study sheds light on the significance of IAM policies and the potential dangers that can arise from misconfiguration.

Encryption and Key Management: Encryption is absolutely necessary for the protection of sensitive data both while it is being transferred and while it is being stored. As per the research [13] examines the encryption mechanisms made available by AWS. These mechanisms include encryption for the AWS Key Management Service (KMS) and the Amazon Simple Storage Service (S3). In the study, both the advantages and disadvantages of using encryption are analysed, and a strong emphasis is placed on the utilisation of safe procedures for managing keys.

Network Security: The Amazon Web Services (AWS) network security model includes a variety of features, including virtual private clouds (VPCs), security groups, and network access control lists (NACLs), among other things. According to [14] analyse the efficacy of the network security policies offered by Amazon Web Services (AWS) in preventing distributed denial-of-service assaults (DDoS). The research sheds light on the optimal configuration procedures that should be followed to protect against attacks of this nature.

Logging and Monitoring: Efficient logging and monitoring are essential components of an effective incident detection and response system for information security. The possibilities of centralised logging and monitoring are investigated in [15] study, which focuses on Amazon Web Services (AWS) CloudTrail and Amazon CloudWatch. According to the findings of the study, it is critical to make use of services like these in order to improve visibility into user activity and detect potential security breaches.

Compliance and Auditing: Amazon Web Services is committed to adhering to a wide variety of compliance standards in order to fulfil the requirements of a variety of sectors. The General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA) are some of the compliance frameworks that are applicable to Amazon Web Services (AWS) [16] that investigates these compliance frameworks.

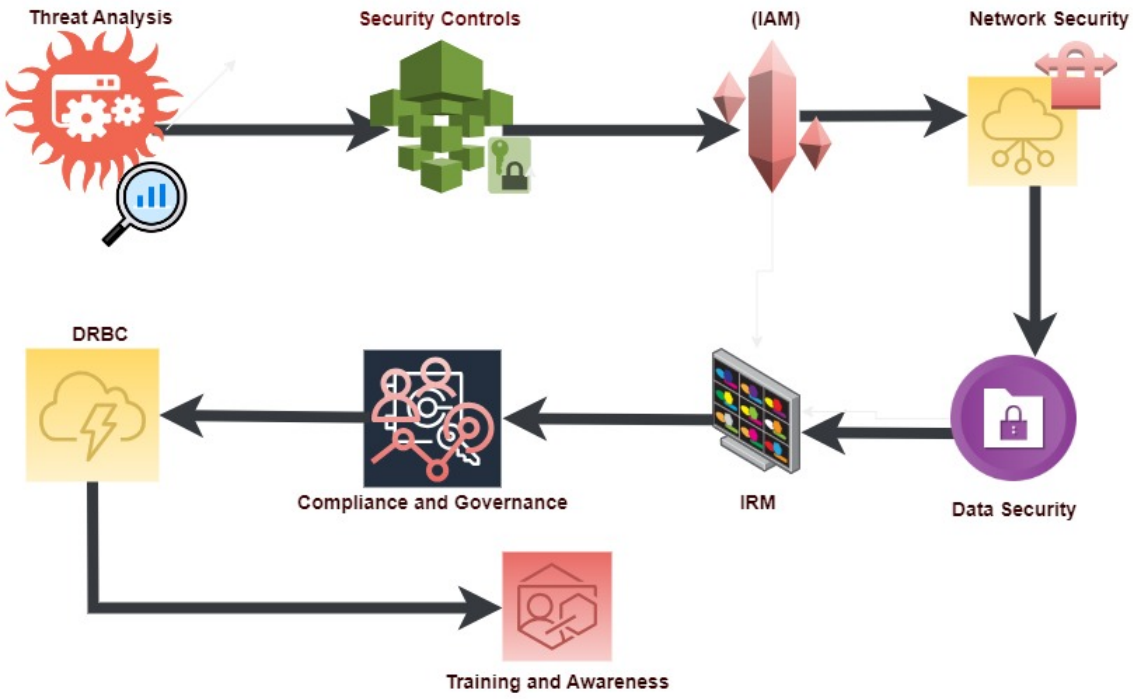
The research emphasises the significance of compliance in protecting the privacy of customer information and guaranteeing its security.

This literature review presents a summary of the research that has previously been conducted on the security model of AWS. The findings provide light on how important AWS security architecture, Identity and Access Management, encryption, network security, logging and monitoring, and compliance are. According to the studies that were looked at, correct configuration, secure key management, and strict adherence to compliance standards are three of the most important things that can be done to reduce possible threats and improve the security of AWS settings. Organisations that utilise AWS services to protect their data and infrastructure in the cloud absolutely need to understand and apply these security procedures in order to maintain adequate levels of protection.

4. Methodology

The systematic procedures that are used to collect and analyse data for a study are referred to collectively as "research methods". Choosing a study design, collecting data, analysing the data using proper techniques, and interpreting the findings are all part of the process.

Figure 1: AWS Security Methodology



Research methodology inherently involves addressing both the existence of constraints and the presence of ethical considerations.

Step 1: Threat Analysis

a. Conduct a thorough analysis of potential threats to the AWS infrastructure.
b. Identify common attack vectors, including network-based attacks, application-level attacks, and insider threats.
c. Evaluate the impact and likelihood of each threat to determine priority levels.

Step 2: Security Controls

a. Identify and describe the various security controls provided by AWS to protect the infrastructure and customer data.
b. Categorize the controls into different layers, such as physical, network, host, application, and data.
c. Explain the purpose and functionality of each control in mitigating specific threats.

Step 3: Identity and Access Management (IAM)

a. Explain the IAM framework provided by AWS for managing user identities and access permissions.
b. Describe how IAM policies, roles, and groups are used to enforce access control.
c. Discuss best practices for implementing strong authentication mechanisms, such as multi-factor authentication (MFA).

Step 4: Network Security

a. Describe the network security measures provided by AWS, including virtual private cloud (VPC), security groups, and network access control lists (ACLs) [17].
b. Explain how VPCs enable logical isolation and segmentation of resources.
c. Discuss strategies for securing network traffic using encryption, VPNs, and AWS Direct Connect.

Step 5: Data Security

a. Discuss the data security features and services offered by AWS, such as encryption at rest and in transit.
b. Explain the use of AWS Key Management Service (KMS) for managing encryption keys [18].
c. Describe how AWS supports compliance with various data protection regulations, such as GDPR and HIPAA.

Step 6: Incident Response and Monitoring

a. Explain the AWS incident response process, including detection, investigation, containment, eradication, and recovery.
b. Discuss the use of AWS CloudTrail for auditing and tracking API activity.
c. Describe how AWS CloudWatch and AWS Config can be used for real-time monitoring and automated remediation.

Step 7: Compliance and Governance

a. Describe the compliance programs and certifications available for AWS services.
b. Explain the shared responsibility model, outlining the responsibilities of both AWS and the customer.
c. Discuss the importance of continuous compliance monitoring and third-party audits.

Step 8: Disaster Recovery and Business Continuity

a. Explain the AWS disaster recovery strategies and services, such as backup and restore options, multi-region deployments, and Amazon S3 replication.
b. Discuss the use of AWS CloudFormation and AWS Elastic Beanstalk for automated deployment and scaling of applications in a resilient manner.
c. Highlight best practices for designing fault-tolerant architectures on AWS.

Step 9: Training and Awareness

a. Emphasize the significance of security awareness and training for AWS users.

b. Provide resources and recommendations for users to stay updated on the latest security practices and guidelines.
c. Discuss the AWS Well-Architected Framework and Security Best Practices documentation.

The technique described above serves as a high-level blueprint for the process of establishing an AWS security model. The actual implementation could be different depending on the precise organisational needs that are being met as well as the AWS services that are being used.

5. Discussions

Amazon Web Services' (AWS) security model is comprised of a comprehensive collection of practises, controls, and technologies. These were developed with the intention of protecting the confidentiality, integrity, and availability of client data and resources while they are stored in a cloud environment managed by AWS. This security model is constructed using a number of essential components, and it employs a multi-layered approach, both of which are designed to offer powerful protection against potential vulnerabilities and threats. During the course of this conversation, we are going to delve into the methodology behind the AWS security model in great detail.

5.1. A Model of Responsibility

The Shared Responsibility Model serves as the cornerstone around which the AWS security methodology is built. Customers are responsible for safeguarding their own apps and data that are operating on Amazon Web Services (AWS), according to this model. Amazon Web Services (AWS) is responsible for the security of the underlying cloud infrastructure. This collaborative approach to security, in which AWS and its customers work together to develop and maintain a safe environment, is made possible by the shared responsibility that exists between them.

5.2. Physical Security

Amazon Web Services continues to place a significant emphasis on the implementation of physical security measures to safeguard its data centres and infrastructure. Access to the AWS facilities is carefully monitored and managed using a variety of security measures, including biometric scanning, video surveillance, and on-site security staff who are present around the clock. In addition, there are redundant power systems, fire suppression devices, and environmental controls in place to assure the safety of customer data as well as its availability.

5.3. Network Security

Amazon Web Services protects data while it is in transit by utilising various layers of network security. This includes isolating customer networks using Amazon's Virtual Private Cloud (VPC), which gives customers the ability to build their own private virtual networks and regulate traffic over those networks. In addition, Amazon Web Services (AWS) offers capabilities such as network access control lists (ACLs), security groups, and so on to manage incoming and outgoing traffic. In addition, Amazon Web Services (AWS) provides customers with Virtual Private Network (VPN) and Direct Connect services, which enable customers' environments to connect safely and securely to AWS.

5.4. Identity and Access Management (IAM)

Identity and Access Management (IAM) is an essential part of the security model used by AWS. Customers are given the ability to properly manage user identities and access privileges thanks to this

feature. IAM makes it possible to create unique user identities, to delegate particular permissions, and to establish multifactor authentication (MFA), which adds an additional layer of security. IAM roles make it possible to implement fine-grained access control, which in turn enables users and apps to access only the resources that they actually require.

5.5. Data Encryption

AWS places a great emphasis on strong data encryption practises in order to safeguard data both while it is at rest and while it is in transit. Customers have the ability to generate and maintain encryption keys through the use of the AWS Key Management Service (KMS), which also provides granular control over the encryption of data. Amazon Web Services (AWS) is able to encrypt data that is kept in a variety of storage services, such as Amazon S3 (Simple Storage Service), Amazon EBS (Elastic Block Store), and Amazon RDS (Relational Database Service). In addition, data transfer capabilities that are encrypted using SSL/TLS protocols are available through AWS.

5.6. Extensive Monitoring and Logging Capabilities

In order to detect and respond to any security events that may occur, AWS provides extensive monitoring and logging capabilities. API activity is logged by AWS CloudTrail, and the resulting audit logs can be put to use for a variety of purposes, including compliance monitoring, auditing, and problem solving. Customers are given the ability to collect and analyse log data from a variety of AWS services through the use of Amazon CloudWatch. This opens the door for real-time monitoring and alerts. Additionally, Amazon Web Services (AWS) provides services such as Amazon GuardDuty, which detects intelligent threats, and Amazon Inspector, which does automate security audits.

5.7. Compliance and Assurance

Amazon Web Services (AWS) keeps a firm commitment to compliance and offers its clients a wide variety of resources to assist them in meeting the specific regulatory standards that are applicable to their businesses. AWS is subjected to routine third-party audits and certifications, such as SOC 1, SOC 2, PCI DSS, and ISO 27001, which serve to demonstrate the company's compliance with standard best practises in the industry. AWS also provides clients with access to compliance tools, like as whitepapers, reports, and security controls matrices, to aid them in their own attempts to comply with relevant regulations.

5.8. Automated Incident Response and Management

In the event that a security breach occurs, Amazon Web Services (AWS) implements a comprehensive incident response strategy to reduce the severity of the disruption and resume business as usual. AWS makes use of automation and machine learning technologies in order to monitor for and react to security events as they occur in real time. In addition, Amazon Web Services offers its customers several tools and services.

To protect its cloud infrastructure and services, AWS continually updates its security model to account for emerging dangers. The future security paradigm of AWS will be determined by a number of important factors. Following can be consider:

a. **Advanced Threat Detection and Prevention:** As cyber threats become more sophisticated, AWS will certainly invest in these methods. Machine learning and artificial intelligence can analyse

massive volumes of data and find anomalies or security breaches in real time. To combat changing threats, AWS may build more proactive and predictive security measures.

b. **Improved Data Encryption:** AWS currently offers strong data encryption. AWS may prioritise encryption as data privacy requirements tighten and data breaches become more sophisticated. To safeguard data at rest and in transit, encryption methods, key management, and secure hardware components may be improved.

c. **Identity and Access Management (IAM) Improvements:** AWS security relies on IAM to fine-tune user access and permissions. AWS may provide more granular IAM features to give organisations more control over user identities, access controls, and authentication processes. Biometrics and multi-factor authentication may be used.

d. **Compliance:** Many organisations must follow industry-specific rules. AWS will likely increase its compliance portfolio to meet changing industry and geographic regulations. Additional certifications, compliance papers, and sector-specific security features may be required.

e. **Continuous Monitoring and Auditing:** Cloud infrastructures need real-time monitoring and auditing to detect and mitigate security incidents. AWS may provide more logging, analysis, and reporting tools to improve monitoring and auditing. Advanced analytics and machine learning could detect suspicious activity and automate incident response.

f. **DevSecOps Integration:** AWS security will integrate further with DevOps. AWS promotes a security culture and helps developers build secure apps by incorporating security policies and practises throughout the software development lifecycle. During development, tools and services may automate security checks, vulnerability assessments, and secure code scanning.

g. **Advanced DDoS Protection:** DDoS attacks continue to threaten internet services. Scalable infrastructure, traffic analysis, and machine learning algorithms will help AWS detect and mitigate DDoS attacks. To remain ahead of DDoS attack vectors, industry partners and global threat intelligence may be needed.

h. **Security Automation and Orchestration:** Complex and dynamic cloud systems require security automation and orchestration for efficiency and effectiveness. Automated security controls, incident response procedures, and security policy enforcement are likely AWS priorities. AWS security services could be integrated with third-party security automation solutions or developed with native automation features.

i. **Enhanced Container Security:** Containerization is popular for deploying programmes in a scalable and segregated manner. AWS may improve container image scanning, runtime security, and vulnerability management. This provides full security controls and visibility for containerized workloads, especially in multi-tenant situations.

j. **Collaborative Security:** As cloud use grows, AWS may support increased collaboration between customers, AWS, and the security community. Sharing threat knowledge, best practises, and

cooperative security exercises can improve security. To help customers and partners secure environments, AWS may expand its security training and certification programmes.

Over all the AWS's security model will focus on staying ahead of emerging threats, improving encryption and access control, meeting compliance requirements, integrating security into DevOps practises, automating security processes, and collaborating with customers and the security community. AWS provides a secure and trusted cloud computing platform by constantly enhancing its security model.

7. Conclusion

In conclusion, AWS's security strategy protects the confidentiality, integrity, and availability of customer data and applications housed on the cloud platform. AWS protects customers using physical, operational, and technical measures. Shared accountability is a strength of the AWS security approach. AWS secures the data centres, networking, and hardware, while clients secure their applications, data, and user access. This shared responsibility model allows AWS and its clients to collaborate on cloud security. AWS secures its data centres physically. 24/7 monitoring, access restrictions, and surveillance systems restrict facility access to authorised staff. AWS data centres are globally spread for redundancy and resilience against natural disasters and service outages. AWS protects customer data with industry-leading operations. Audits, compliance certificates, and thorough staff screening are included. AWS offers HIPAA, PCI DSS, and ISO 27001 compliance programmes to assist companies fulfil data security regulations. AWS's security tools and services can help customers improve their security. Identity and access management (IAM) controls user permissions, network security groups (NSGs) configure firewalls, and virtual private clouds (VPCs) isolate networks. AWS encrypts data in transit and at rest. The AWS Trusted Advisor regularly analyses customers' accounts and recommends security setting optimisation and vulnerability detection. This proactive approach protects clients from security breaches. AWS invests extensively in security R&D to stay up with evolving threats and industry best practises. The AWS Security Incident reaction Team (SIRT) monitors and responds to security occurrences, providing a quick and effective reaction. AWS security protects customer data and applications. AWS creates a secure cloud environment that allows organisations to confidently use the cloud while lowering security risks by combining physical, operational, and technical safeguards with customer responsibility. AWS is a trusted cloud platform for businesses of all sizes due to its robust security and ongoing advancements.

References

1. S. Bhatt, T.K. Pham, M. Gupta, J. Benson, J. Park and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future", IEEE Access, vol. 9, no. 1, pp. 107200–107223, 2021. https://doi.org/10.1109/access.2021.3101218
2. Md. S. Shams, A.A. SM, A.M. Sattar and M. Ranjan, "Study and Analysis of Components and Impact of AWS on Cloud Computing", Recent Trends in Parallel Computing, vol. 10, no. 1, pp. 35–42, 2023.
3. S. Bhatt, T.K. Pham, M. Gupta, J. Benson, J. Park and R. Sandhu, "Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future", IEEE Access, vol. 9, no. 1, pp. 107200–107223, 2021. https://doi.org/10.1109/access.2021.3101218

4. Patrícia Pelufo Silveira, A. Triano, J. Verdu and Pedro de Paco, “Complex Terminating Impedance for AW Filters: The Key for Power Amplifier Co-design”, October 2019, https://doi.org/10.1109/ultsym.2019.8926248
5. I. Zinno et al., “National Scale Surface Deformation Time Series Generation through Advanced DInSAR Processing of Sentinel-1 Data within a Cloud Computing Environment”, vol. 6, no. 3, pp. 558–571, September 2020. https://doi.org/10.1109/tbdata.2018.2863558
6. S. Bhatt, T.K. Pham, M. Gupta, J. Benson, J. Park and R. Sandhu, “Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future”, IEEE Access, vol. 9, no. 1, pp. 107200–107223, 2021. https://doi.org/10.1109/access.2021.3101218
7. M.D. Boomija and S.V.K. Raja, “Securing medical data by role-based user policy with partially homomorphic encryption in AWS cloud”, Soft Computing, March 2022. https://doi.org/10.1007/s00500-022-06950-y
8. M. Hazaryan, M. Salehi Kamboo, F. Mirzaeipour and R. Maasoumi, “Observance of Patients’ Rights by Physicians and Operating Room Technicians”, Medical - Surgical Nursing Journal, vol. 10, no. 4, February 2022. https://doi.org/10.5812/msnj.123316
9. A. Pandit, S. Sawant, R. Agrawal, Jayantrao Mohite and Srinivasu Pappula, “A Scalable Automated Satellite Data Downloading and Processing Pipeline Developed on AWS Cloud for Agricultural Applications”, pp. 139–152, March 2023. https://doi.org/10.1201/9781003270928-10
10. D. Clinton and B. Piper, “Amazon Virtual Private Cloud”, in AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, Wiley, pp. 83–132, 2021.
11. M. Gupta, J. Benson, F. Patwa and R. Sandhu, “Secure V2V and V2I Communication in Intelligent Transportation using Cloudlets”, IEEE Transactions on Services Computing, pp. 1–1, 2020. https://doi.org/10.1109/tsc.2020.3025993
12. B. Piper, AWS Certified Solutions Architect Study Guide : Associate SAA-C02 Exam with Online Labs. S.L.: Wiley-Sybex, 2021.
13. X.-L. Huang and R. Chen, “A Survey of Key Management Service in Cloud”, November 2018. https://doi.org/10.1109/icsess.2018.8663805
14. S. An, A. Leung, J.B. Hong, T. Eom and J.S. Park, “Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security”, IEEE Access, vol. 10, pp. 75117–75134, 2022. https://doi.org/10.1109/access.2022.3190545
15. D. Sun, M. Fu, L. Zhu, G. Li and Q. Lu, “Non-Intrusive Anomaly Detection With Streaming Performance Metrics and Logs for DevOps in Public Clouds: A Case Study in AWS”, IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 2, pp. 278–289, April 2016. https://doi.org/10.1109/TETC.2016.2520883
16. M. Kellogg, M. Schäf, S. Tasiran, M.D and Ernst, “Continuous Compliance”, 2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE), Melbourne, VIC, Australia, pp. 511–523, 2020.
17. M. Neto et al., “Security Troubleshooting on AWS”, “Security Troubleshooting on AWS”, in AWS Certified Security Study Guide: Specialty (SCS-C01) Exam Wiley, pp. 339–362, 2021. https://doi.org/10.1002/9781119658856.ch9
18. X.-L. Huang and R. Chen, “A Survey of Key Management Service in Cloud”, November 2018. https://doi.org/10.1109/icsess.2018.8663805