WHITE PAPER

SECURING MICROSERVICES ON AWS – A GUIDE FOR FS FIRMS

Abstract

Application security is a core functional requirement for every Financial Services firm. To protect their applications, resources and customer data from potential threats and exploitations, designing and building secure applications on the cloud is of paramount importance. FS firms need to explore best strategies to achieve the security objectives for their business-critical applications on the cloud. Amazon Web Services (AWS) is best suited for this as it provides stringent security services and features to secure applications, resources and data. This whitepaper provides an overview of key cloud security challenges along with best practices to ensure secure microservices applications on AWS.

Infosys®
Navigate your next

Introduction

Over the past few years, as Financial Services (FS) firms have been steadily adopting cloud services to drive their business forward, the rate of microservices adoption in the cloud is growing at a rapid pace. We describe microservices as independent services which are distributed over different networks and communicate over well-defined APIs modelled around a business domain. It's an architectural approach to develop software with benefits of faster development cycle, scalability, increased agility, productivity, enabling innovation and accelerating time-to-market for new features. To leverage these benefits, FS firms across the globe have already started adopting microservices and are moving from On-Premises to Cloud.

Application security issues and threats are a major challenge to FS firms as they process and transmit highly sensitive customer information and financial data over their networks. They need the best-in-class security strategies to secure their applications from web exploits and threats such as SQL injections, man-in-the-middle attacks, sensitive data exposure, SSRF, DDoS, etc. To address these security issues, and protect applications and data on the cloud, they need a highly secure infrastructure and secure services.

Securing microservices on the cloud is a challenge for FS firms due to the number of distributed components and larger attack surface, security issues, regulatory and compliance concerns. Traditional security systems do not provide adequate security mechanisms to protect microservices, data and infrastructure on the cloud. The Amazon Web Services (AWS) is a cloud platform that provides one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable and highly reliable platform that enables customers to deploy applications and data quickly and securely. Using AWS API Gateway, Cognito, IAM and CloudWatch services, FS firms can secure applications, APIs and data at any scale to meet their security objectives.

Security for Financial Services on the cloud

The Need for a Stringent Security system

FS firms across the world store, process and transmit customers sensitive information such as customer bank account data, credit card data, personal data, SSN etc. for business requirements. In a microservices architecture, a large number of components are distributed and sensitive customer data flows through different components and systems over the network. It's not an easy task for FS firms to adopt the cloud and secure sensitive data and applications on the cloud.

Without a proper security mechanism on the cloud, it increases security risk and issues such as sensitive data exploitations, data breaches, man-in-the-middle attacks, SQL injections, cross-site scripting, DDoS, etc. These attacks are increasing due to misconfiguration, unauthorized applications access, insecure APIs, cyber-attacks, etc. which severely harm financial firms and customers. Hence, FS firms need a better strategy to implement the stringent security system on the cloud to secure microservices applications and data.

Key Challenges and Security Issues

Application security issues have been a challenge for FS firms for years. They face various challenges, security issues and concerns while adopting the cloud and securing microservices applications.

Key challenges

- *Security and data privacy issues*
- *Regulatory and compliance challenges*
- *Lack of clear security strategy for cloud*

As per the 2020 checkpoint, the biggest contributors to cloud security threat is misconfiguration (68%), followed by unauthorized access (58%), insecure APIs (52%) and others as depicted in the diagram.

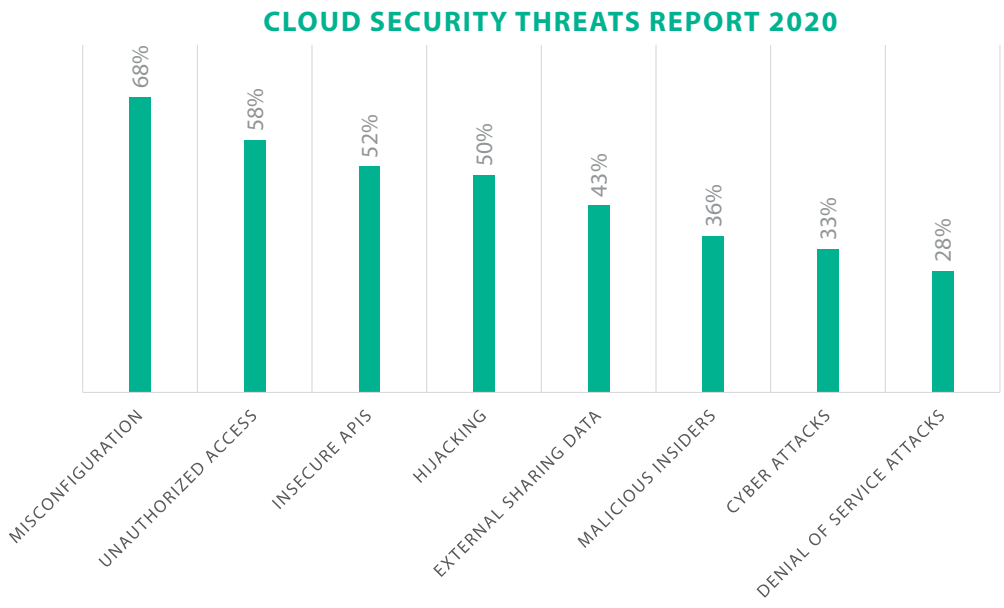

Figure 1 : Security threats report

In 2019, Capital One was fined $80 million for a hack of 100 million credit card data of customers. The security threats happened due to misconfiguration in AWS environments and unauthorized access. Hence, it's vital for FS firms to build a robust security system on the cloud.

Strategy to Resolve Security Challenges & Issues

In order to resolve security challenges and issues, we recommend a better strategy which FS firms can adopt to secure microservices applications on AWS. This approach includes:

- Understanding security challenges and issues
- Selecting the best cloud service provider
- Understanding the shared responsibility model
- Designing security by applying the best approaches
- Implementing security on the cloud by applying best practices

As security requirements vary from application to application, FS firms need to understand the strategy along with AWS security model, services and features to overcome the key security issues, concerns and challenges.

AWS Security: Shared Responsibility Model

Security on AWS is a shared responsibility between AWS and the customer. It is very important for FS firms to understand the Shared Responsibility Model (SRM) while designing security for microservices on AWS. AWS is responsible for security of the cloud and the FS organization is responsible for security in the cloud.

- AWS is responsible for protecting the infrastructure, compute, storage, database, network, hardware and software on the AWS environment.
- The FS firm is responsible for protecting data, IAM access, firewall and network configurations, encryptions, etc. The SRM is summarized in the below diagram.

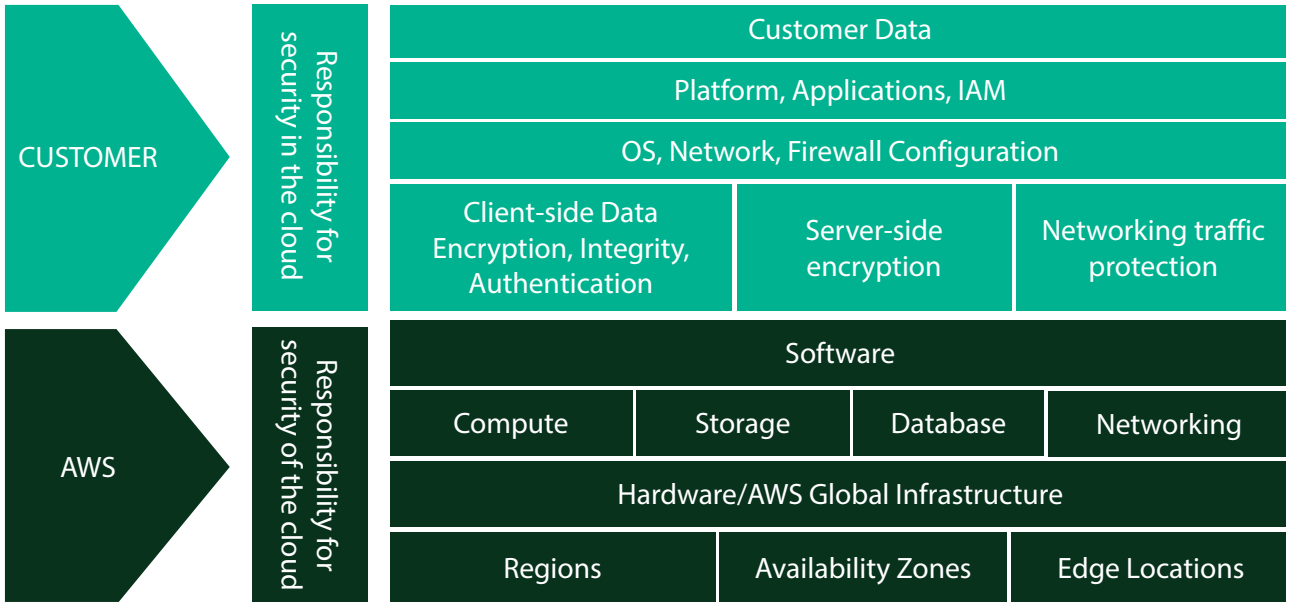

Figure 2 : AWS Shared responsibility model

Security by Design Approach

Security by Design (SbD) is an approach to design security and compliance capabilities for all phases within the AWS environment. AWS SbD provides increased capability for designing end-to-end security for all services, data, and applications in AWS. FS firms can leverage AWS SbD approach while designing security and compliance capabilities for microservices applications.

SbD recommends a four-phase approach to design a robust security environments on AWS.

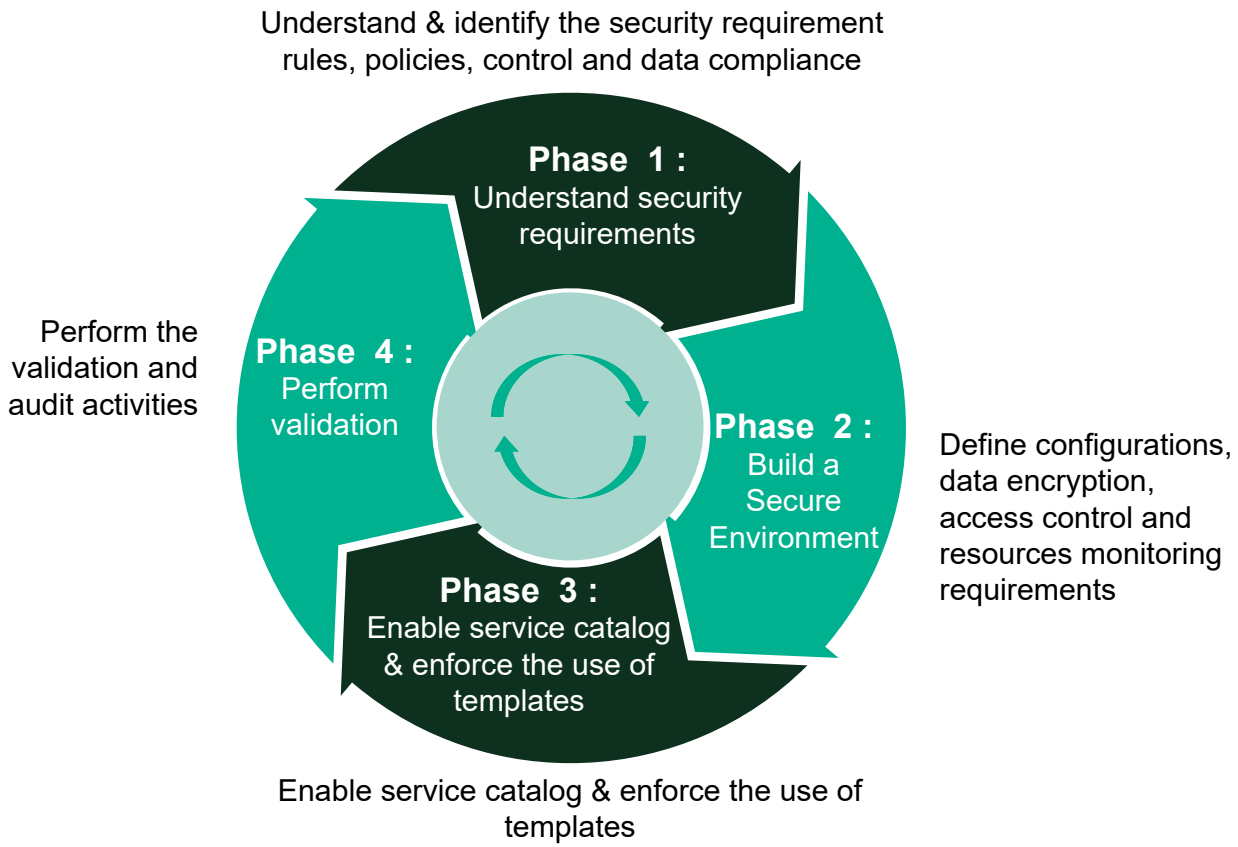

Figure 3 : SDB phases

AWS: Defense in Depth

We describe Defense in Depth (DiD) as a mechanism to apply layers of security countermeasures to protect applications, services and data. The goal of this approach is to identify the applications and services with the most customer sensitive information and apply multiple security layers to protect them. The best way to achieve DiD on AWS is summarized below:

- Leverage AWS WAF (Web Application Firewall) features to build and configure multi-layer security for applications.
- Use AWS Managed Rules Core Rule Set (CRS) to protect the inner application layer and AWS CloudFront with Shield to enforce security in the outer layer of application.
- For application specific issues like SQL injection, it is best to use AWS managed rules in application layer policy enforcement.
- Use Amazon Machine Image (AMI) for third-party web application firewall layer policy enforcement.
- Use private layer policy enforcement to deploy an application load balancer in a private subnet serving web front ends.
- Create a layered solution for network security using Amazon VPC, implicit firewall rules, network access control list, security groups, host-based firewalls and IDS/IPS system.

Secure APIs via AWS API Gateway

Generally, microservices consist of serval components which are distributed over different networks and expose APIs to the public. The services can be accessible from a wide range of systems and clients. Exposing APIs to public increases security risks and issues for FS firms.

- The solution to avoid security issues is to create a single secure entry point called API Gateway. The API Gateway acts as an entry point for all the external client requests, systems and efficiently hides microservices from client direct access
- With client and external systems having no direct access to microservices, no service can be exploited
- FS firms can leverage AWS API Gateway features to create, publish, maintain, monitor, and secure APIs at any scale.

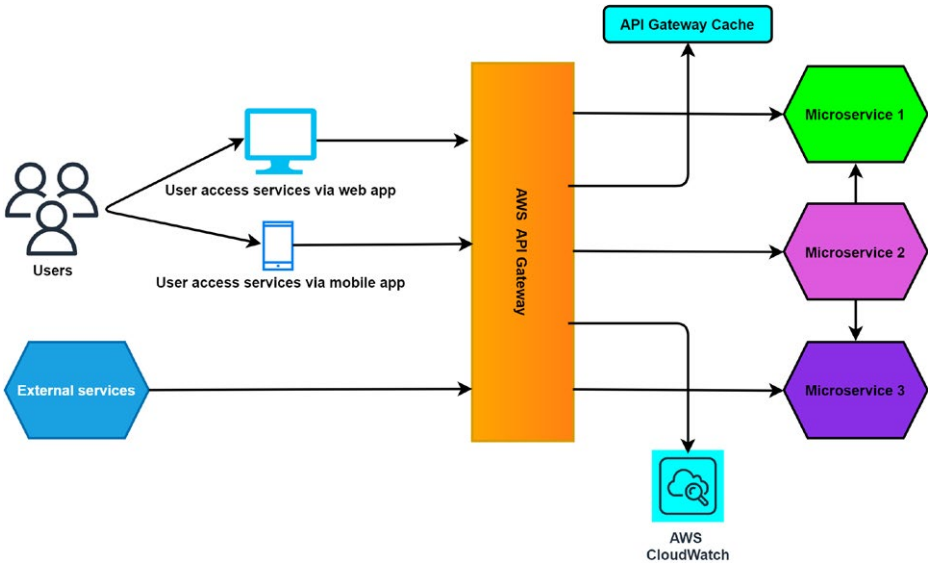

Figure 4 : AWS API Gateway architecture to secure microservices

Secure Microservices via IAM

FS firms need a robust access control system to secure their applications and resources on the cloud. AWS provides Identity and Access Management (IAM) service to securely manage access to AWS services and resources. To manage access, AWS supports six types of security policies such as identity-based policies, resource-based policies, permission boundaries, Organizations SCPs, ACLs, and sessions policies.

Using IAM, FS firms can create and manage users and groups, allowing access control permissions for microservices and resources on AWS.

Secure Microservices users via AWS Cognito

FS firms need a secure authentication, authorization and user management system to protect microservices from unauthorized access and exploitations.

- To address these security issues, AWS Cognito provides authentication, authorization and user management services to protect microservices. AWS Cognito has user pools to authenticate users and identity pools to grant user access to microservices and other AWS Services.

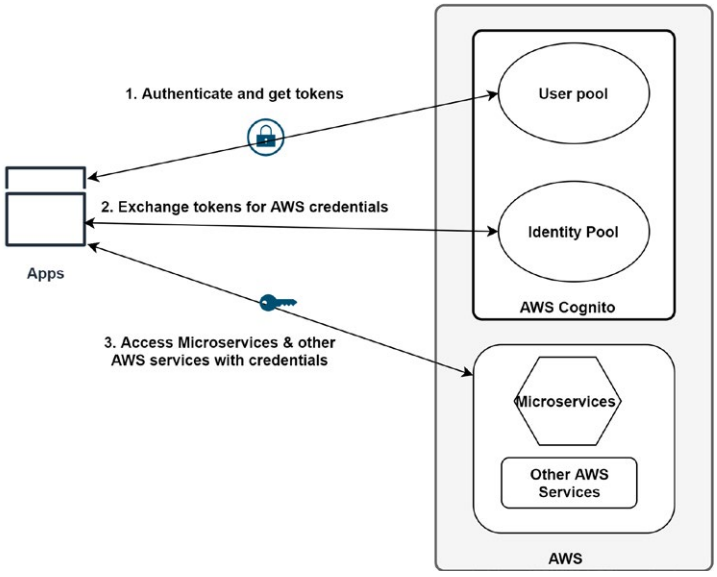

Figure 5 : AWS Cognito Authentication Architecture Diagram

Security features of Cognito:

- Provides secure and scalable user directory called Cognito User Pools
- Provides standard-based authentications and supports Oauth2.0, SAML 2.0 and Open ID
- Supports multiple-factor authentication and encryption of data-at-rest and in-transit
- It is HIPAA eligible and PCI DSS,SOC,ISO/IEC 27001,ISO/IEC 27017,ISO/IEC 27018 and ISO 9001 complaint

Best Practices for Securing Microservices on AWS

API Gateway

- Implement least privilege access using IAM policies for controlling and managing permission and access for microservices
- Enable encryption and content encoding features
- For http backend authentication, use client-side SSL certificates
- Rotate expiring SSL client certificates periodically
- Secure API Gateway APIs from common web exploits using AWS WAF
- Use AWS CloudWatch for logging & monitoring and enable AWS X-Ray for tracing
- Enable AWS CloudTrail to record user actions
- Enable AWS Config & SNS to secure configuration of AWS resources

Resources Configuration

- Configure and allow authorized users to access and manage microservices on EC2
- Do not allow large IP ranges from inbound access to EC2 and do not allow large ranges of port opens for EC2 security groups
- Configure secure SSL ciphers and SSL/TLS certificates for secure connections
- Rotate SSH keys periodically and delete not-in-use keys

IAM Authentication Best Practices

- Use a strong password to protect the AWS root account and management console
- Configure and set up a strong password policy for IAM users, group and roles
- Enable multi-factor authentication for the AWS root account
- Use AWS secrets Manager for storing database passwords
- Grant least privilege and rotate security credentials regularly

Data Protection

- Use AWS key management service to protect data across microservices
- Encrypt data in transit for all network traffic
- Use AWS Secrets Manager service to store and manage application credentials securely
- Use AWS Certificate Manager service to manage public and private SSL/TLS certificates securely
- Encrypt data at rest by encrypting EBS volumes and S3 buckets
- Use AWS Quicksight to provide data access to business users and remove unnecessary access to the database

IAM Access Control

- To manage each service, create user groups for each service and set up IAM policies to manage and control access permissions for applications and data
- Enable MFA to control access to AWS service APIs
- Avoid programmatic access to AWS resources using access keys associated with the root account
- Rotate IAM access keys on regular basis and remove not-in-use access keys

Secure Infrastructure

- Configure and use AWS CloudFront, WAF and Shield to protect from DDoS attacks
- Enable AWS systems patch manager to automate OS patching activity and application code-related updates
- Configure security groups to control inbound and outbound network traffic

Secure Operating Systems and Applications

- Disable root API access keys and secret key
- Configure to restrict access to instances from limited IP ranges using Security Groups
- Protect the .pem file on user machines
- Delete keys from the authorized keys file on instances when someone no longer requires access
- Rotate credentials (DB, Access Keys)
- Regularly run least privilege checks using IAM user Access Advisor and IAM user Last Used Access Keys
- Use bastion hosts to enforce control and visibility

Cognito

- Enable multi-factor authentication to the user pool to protect the identity of users
- Configure advance security for the user pool to block malicious attempts and for credentials
- Enable CloudWatch for auditing user pool data

Monitoring and Auditing

- Enable AWS CloudTrail for monitoring and tracking all the activities of microservices
- Enable CloudWatch and GuardDuty to monitor and track threat detection, malicious activity and unauthorized behavior
- Enable logging using CloudTrail at both application and service level
- Enable AWS Config to audit configuration changes in all accounts and regions where microservices are deployed

Example Use case for Financial Services

Capital One is a leading Financial Corporation of the US providing banking and financial services such as credit cards, checking and savings accounts, auto loans, rewards, and online banking services to customers and businesses. However, the bank faced a massive data breach security issue in 2019 and was fined $80 million.

Post this breach, they decided to use AWS services, the security model, and expanded use of microservices. The organization has built a stringent security system using AWS services and features along with best approaches and practices to protect applications and data on the cloud. Due to the stringent security system, the bank announced going All-in on the cloud. Today the bank has resolved all security threats on the cloud and serves its customers better and implements innovative ways to increase revenue.

AWS Benefits for Financial Services

Figure 6 : AWS Security benefits

Conclusion

AWS provides robust security services and features to secure microservices and data on the cloud. FS firms need to understand the Shared Responsibility Model along with best services, approaches and practices to protect their applications on AWS. The key recommendations are summarized below:

- *Understand security requirements for applications*
- *Identify the security issues and challenges*
- *Design applications by applying AWS best security practices to countermeasure the security issues*
- *Enable AWS services and use the best tools to secure applications and data on the cloud*

As more and more FS firms are adopting microservices in the cloud, security issues and threats will remain a challenge for them. However, these security issues can be prevented by adopting best-in-class and highly secure cloud services along with the best strategy, approaches and practices.

About the author

Ananta Kumar Behera, *Technology Lead, Infosys*

- Over 9.5 years of IT experience with exposure to Finance domain and Java/J2EE, Spring, Microservices technologies
- Passionate about learning new skills and currently focusing on learning new digital and cloud technologies

References

http://aws.amazon.com/compliance/security-bydesign

https://aws.amazon.com/architecture/security-identity-compliance/

https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

https://docs.aws.amazon.com/apigateway/latest/developerguide/security-best-practices.html

https://docs.aws.amazon.com/cognito/latest/developerguide/managing-security.html

https://pages.checkpoint.com/2020-cloud-security-report.html

https://aws.amazon.com/solutions/case-studies/capital-one-enterprise/

https://www.washingtonpost.com/national-security/capital-one-fined-2019-hack/2020/08/06/90c2c836-d7f3-11ea-aff6-220dd3a14741_story.html

https://cipher.com/blog/analysis-cyber-attack-capital-one/

https://aws.amazon.com/solutions/case-studies/capital-one-all-in-on-aws/

For more information, contact askus@infosys.com

Infosys®
Navigate your next