Merrilton Banking

Cloud-Based Banking Solution

Cloud Architecture – D088

Nicholas Ortiz

04/29/2021

[Version 1.0.6]

WESTERN GOVERNORS UNIVERSITY

Table of Contents

A. Propose of Authentication Process

All user and device authentication will be handled by Amazon AWS Cognito with User Pools. This enables the user of device mappings to user while also limiting the number of registered devices per users. When a user reaches their account's limit, they must access their account using a known devices to unregister unused devices in order to reduce the number of registered devices on their account. [CITATION Placeholder2 \l 1033]

When a user accesses their account from an unregistered devices using their user credentials, AWS Cognito with User Pools will prompt them for additional verification via SMS or a Time-based One-time Password (TOTP) generator using a compatible mobile authenticator application (e.g. Google Authenticator, Authy). If the user has not yet installed a compatible mobile authenticator application, they must have a registered cell phone in order to receive an SMS text message containing their Time-based One-time Password. [CITATION Ama214 \l 1033]

When a user attempts to access the bank's resources from an unknown browser or devices, the additional verification requirements will be triggered. The international mobile equipment Identity number will be used to determine whether the devices is new or previously registered, as well as to link the user to their account.

B. End-to-end encryption solution between the application and the cloud

Due to the added level of security of such devices, remote access by employees will be performed by Multi-factor Authorization (MFA), with a dynamic token used as the second verification criteria. All employees will be given a Yubikey for remote access, and the dynamic token will provide the credential required for MFA to be accepted. [CITATION Placeholder1 \l 1033]

When a user accesses the bank's resources remotely, they will be prompted for their Yubikey credentials after entering their username and password. When prompted, the user will insert their Yubikey into a USB port on the computer and press the configured keyboard key to pass the credentials to the MFA login screen.

If the employee accesses the bank's resources via a mobile devices, the Yubikey supports Near-Field Communication (NFC) to pass the Yubikey criteria to the MFA authentication login. Employee's mobile devices must support NFC technology due to the sensitive nature of their work.

C. End-to-end encryption solution between the home office and the cloud

Conditional access policies enforced with a Trusted Device list manage access to the Merrilton Banking workspace from the home office. To protect all data at rest on the employee's computer and/or mobile devices, conditional access will necessitate 256 AES device encryptions. Data in transit will be protected by a VPN that employs IKEv2 and IPsec [CITATION Tim19 \l 1033]. All access to company resources requires a unique username and password combination, as well as MFA via a company issued FIDO2 compliant Yubikey and the WebAuthn protocol[CITATION Placeholder1 \l 1033]. Finally, policies governing password complexity and user lockout will be implemented.

D. Systems Integration Utilizing Internal and External API Calls

A series of both internal and external APIs will be used to provide a complete end-to-end solution for bank customers and employees.

D.1. Internal APIs

AWS HTTP API, AWS REST API, and AWS WebSocket API will be the primary internal APIs used. All of these will be used in tandem with AWS Lambda for serverless compute functions. Amazon CloudWatch logs will be used to enable robust logging as well.

The following sections go over the specifics of each API.

D.1.1. AWS HTTP API with AWS Lambda

By sending requests to AWS HTTP API, AWS Lambda will be used to provide application access to the cloud resources.[CITATION Ama217 \l 1033] The API will be stored in an AWS API Gateway created through the AWS Gateway Console. After the bank customer or employee enters their username and password into the AWS hosted application login portal, the API will be invoked and will first look for the MFA token. The token is then validated, and if successful, it is passed to the API Lambda function, granting access to cloud resources. [CITATION Ama215 \l 1033]

To address fraud risks, all data logging for the API will be handled by a CloudWatch Logs group and stored in a database for a minimum of one year. The log will record the username, account number, timestamp, login information, errors, and source IP address of the account access login request. All failed login attempts will be routed to the Fraud Department for review and final assessment. [CITATION Ama216 \l 1033]

Depending on whether the fraud alert was triggered by a bank customer or an employee, the Fraud Department will be notified of the following:

Employee alerts

- Timestamp of the alert
- Employee ID of the person accessing the cloud applications
- IP address of the client system accessing the cloud applications
- MFA method used when accessing the cloud applications
- Any account numbers affected by the trigger

Bank Customer alerts

- Timestamp of the alert
- User ID of the person accessing the cloud applications
- The account number of the person accessing the cloud applications
- MFA method used when accessing the cloud applications
- Any account numbers affected by the trigger
- All activity performed within the application that triggered the alert

The Fraud Department and IT SecOps will review all logs at least once every seven days, and the Fraud Department will review, validate, and respond to any alerts within the SLA of four hours.

D.1.2. AWS REST API WITH AWS LAMBDA

Merrilton Bank branch locations will use an API Gateway REST API as a request/response model for applications that require secure synchronous communication. The API will be stored in an AWS API Gateway and will be created through the AWS Gateway Console. It is triggered when an employee accesses a client account that requires immediate feedback of account details for inquires, when the employee performs database lookups for clients, and when the employee performs loan calculations. [CITATION Ama215 \l 1033]

AWS Lambda will convert the data returned from JSON into readable formatted information, which will then be passed to the requesting application. [CITATION Ama217 \l 1033]

A CloudWatch Logs group will record all activity while the employee is interacting with the client account. Employee number, timestamp of access, IP address of source workstation, any transaction performed on the account, and duration of activity will all be tracked.[CITATION Ama216 \l 1033]

Any activity performed that does not have the proper approvals noted in the account will be forwarded to the Fraud Department for review, including but not limited to:

- Suspicious transfers without proper paperwork in place
- Credit increases without proper Credit Score review
- Transfers between accounts that are not linked

D.1.3. AWS WEBSOCKET API WITH AWS LAMBDA

The AWS WebSocket API will be used within the API Gateway for its route capabilities, which will be integrated with AWS Lambda functions and other AWS services. When a bank customer initiates a chat support session with a bank employee, the API is called. It will also be triggered when a bank customer requests an SMS one-time passcode to gain access to their account.

A CloudWatch Logs group will be used to capture all information during the chat session so that it can be emailed to the bank customer once the chat session is finished. The chat session will only be sent to the primary email address associated with the account, and a copy will be saved in a database in case it needs to be reviewed by the Fraud Department. The Fraud Department will be notified of the chat session only if the bank customer initiates a fraud investigation by clicking a link received in the record of the chat sessions transcription.

When a bank customer clicks the fraud investigation link, they will be directed to login to their account and complete a fraud investigation form. When the form is submitted, the AWS WebSocket API is called, which sends an email to the Fraud Department informing them of the fraud investigation request.

When a chat session with a bank employee is started, relevant bank customer information such as first and last name, call bank number, account number, and the first message sent by the bank customer in the chat session is sent in JSON format via AWS WebSocket and translated into relevant data using AWS Lambda Functions. The AWS WebSocket API will then route the chat session to a queue and assign it to a bank employee who is available. When the session is accepted, an AWS Lambda function is used to retrieve the customer's account information. [CITATION Ama215 \l 1033]

D.2. External APIs

Merrilton bank customers will benefit from enhanced functionality while using the cloud application thanks to the use of Google Sign-in for Websites, Google Geolocation API, and Equifax Consumer Data Suite (CDS) Product API.

The sections that follow go over each external API's usage in detail.

D.2.1. Google Sign-In for Websites

Google Sign-in for websites will be used to enable single-sign-on. Because of Google Identity APIs, bank customers will be able to sign in to their accounts using the Google Sign-in button. Google Sign-in requests will generate an ID token after the OAuth 2.0 client sign-in has been properly configured. The ID token will be sent to the backend server via HTTPS POST. To validate the token's integrity against Google's public keys, the Python Google API client library is used. After a successful MFA challenge and response, the aud value of the ID toke is matched to the bank customer's ID, and the bank customer is granted access to their account. [CITATION Ama218 \l 1033]

D.2.2. Google Geolocation API

The Google Geolocation API will be used in the mobile app for both Android and iOS deployments to find the bank customer's nearest branch office. Google will host the API, and after a successful geolocation request, the geolocation data will return a JSON-formatted response, which will be transmitted from the API over HTTPS using POST. This data will be translated and compared to a Merrilton Bank branch location database. A list of the ten closest branch locations, ordered from nearest to farthest, will be returned to the end user's device. [CITATION Goo21 \l 1033]

D.2.3. Equifax Consumer Data Suite (CDS) Product API

Bank customers will be able to view their credit score from the three major credit bureaus by using the Equifax Consumer Data Suite (CDS) Product API. JSON Web Tokens (JWT) are used to secure the CDS Product API for OAuth 2.0 client authentication and authorization. After logging in, bank customers' credit scores will be displayed in their account overview once they have been configured. Customers will be able to set up alerts if there is unusual activity on their credit report, and their scores will be automatically updated. [CITATION Equ20 \l 1033]

E. Deployment plan

The full implementation will take one year from the approved start date. The first month will be devoted to determining which applications and services can be migrated to the cloud. Once this is completed, the cloud deployment team will be contacted to begin spinning up and testing the deployed application in the cloud, and a group of 100 test users will be chosen for quality assurance.

The application development team will start working on mobile apps for Android and iOS that will allow banking customers to access their accounts. All API requirements that must be integrated into the application for security purposes will be provided to the application developers. The application development process is expected to take nine months from start to finish.

Two independent auditing firms will audit the applications, security, and regulatory compliance during the final three months of the implementation plan. Additionally, items flagged by auditors will be addressed and corrected in order to obtain certification compliance with all required regulations.

For the first year, the total cost of project implementation is estimated to be $2 million USD for deployment and migration to the AWS cloud, which will be treated as CapEx. The annual operating cost of AWS services is estimated to be $1.3 million USD in OpEx.

F. Maintenance Strategy

The Change Advisory Board (CAB) will oversee ongoing maintenance to the cloud application and cloud infrastructure. All modifications will be categorized as Low, Normal, High, or Critical. All changes will be prioritized based on their risk to business continuity and must include a fail-safe plan. It is advised to follow the standard ITIL v4 Change Management process.

F.1. Patch Management

Each month, cloud infrastructure will be updated to the most recent patch level in order to maintain a secure environment. Patches will be applied to the Dev environment as a standard change within two days of their release. If no issues are discovered during validation testing, the patches will be applied to the Prod environment as a normal change within 7 days of their release. The severity and impact of out-of-band patches will be assessed. If they are deemed necessary for business continuity, they will be implemented as a critical change in the Dev environment. Validation testing will last two days, after which the patch will be applied to the production environment as a critical change.

F.2. Updates and Redevelopment

The application development team will be in charge of all updates, which will follow a standard DevOps cycle. All application updates will go through the following stages: planning, technical stage, prototyping, development, quality assurance, and publishing. The applications will be maintained indefinitely to ensure that any reported bugs are addressed and resolved in accordance with the aforementioned process. [CITATION Sha17 \l 1033]

On a 60-day rolling Blue-Green update cycle, the application will be updated with new features and bug fixes. Focus groups will test for bugs and end user acceptance of all new functionalities as new functionalities and technologies are released on the current development track utilizing an

application load balance with weighted target groups. The current stable will remain stable until all new features have been certified by the development's quality assurance stage. Once changes are accepted on the current development track, the load balancer will shift all traffic to that track. The track will be re-classified as the stable track and mirrored to both tracks to maintain application continuity. [CITATION Placeholder3 \l 1033]

G. Disaster recovery plan

AWS regions and availability zones will have a business continuity and disaster recovery plan. NetApp Cloud Volumes ONTAP will create SnapShot copies of all resources using Amazon Elastic Block Store (EBS) and Amazon Simple Storage Service (S3).

With SnapMirror integrated technology, this solution will replicate across availability zones, regions, and to and from the datacenter. This enables high availability as well as data replication from the datacenter to AWS for backups. SnapShot creates point-in-time backup and recovery points for all data, allowing for faster recovery times in the event of outages or equipment failure. [CITATION Inb19 \l 1033]

For cloud-based services, AWS Regions and Availability Zones will be used for performance, reliability, security, and scalability. The disaster recovery plan will make use of cloud datacenters in the following AWS regional centers: Northern Virginia, Ohio, and Northern California. In the event of a datacenter failure, the cloud-based VPN router will route all traffic from all branches and remote sites to the HOT copy in the next available region's data center. [CITATION Liv21 \l 1033]

H. Compliance

All FDIC, PCI DSS, SOX, and any other local or governmental laws, regulations, and standards will be followed and implemented for all applications and data. The implementation will be audited quarterly to ensure that all data at rest is encrypted and only accessible to employees who need it for their job. All in-flight data must be encrypted using IKEv2 and IPsec VPN secure connections to the data center and cloud.

Without proper authentication, the primary account number will be stored and rendered unreadable, full track data will not be stored, the CAV2/CVC2/CVV2/CID will not be stored at all, and the PIN/PIN Block will not be stored. An external auditor will review all documents and validate compliance on an annual basis for regulatory compliance.

To ensure compliance with SOX, an independent auditor will perform independent oversight to ensure all aspects comply with all SEC and federal agencies.

For the FDIC, all applicable regulations will be followed, enforced, and audited in accordance with the regulations by an independent auditing firm. [CITATION FDI18 \l 1033] [CITATION Ken20 \l 1033]

References

Amazon Web Services, Inc. (2021). *Amazon API Gateway Developer Guide.* Retrieved from Working with HTTP APIs: https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api.html

Amazon Web Services, Inc. (2021). *Amazon Cognito Developer Guide*. Retrieved from Amazon Cognito user pools: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools.html

Amazon Web Services, Inc. (2021). *TOTP Software Token MFA*. Retrieved from Amazon Cognito Developer Guide: https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-mfa-totp.html

Amazon Web Services, Inc. (2021). *Amazon CloudWatch User Guide.* Retrieved from Working with Log Groups and Log Streams.

Amazon Web Services, Inc. (2021). *AWS Lambda - Serverless Compute - Amazon Web Services.* Retrieved from AWS Lambda: https://aws.amazon.com/lambda/

Equifax Inc. (2020). Consumer Data Suite User Guide 1.0. Atlanta, Georgia, United States of America.

FDIC. (2018, June 29). *FDIC Law, Regulations, Related Acts - Rules and Regulations*. Retrieved from https://www.fdic.gov/regulations/laws/rules/2000-6400.html

Google Developers. (2021, 09 14). *Integrating Google Sign-In into your web app.* Retrieved from Google Identity: https://developers.google.com/identity/sign-in/web/sign-in

Google Developers. (2021, 4 28). *Overview Geolocation API Google Developers.* Retrieved from Google Maps Platform: https://developers.google.com/maps/documentation/geolocation/overview

Inbar, O., Maimoni, A., Cruz, S., & Singh, S. (2019, April). NetApp Cloud Volumes ONTAP with SQL Server on the AWS Cloud. Amazon Web Services Inc.

Kenton, W., & Berry-Johnson, J. (2020, Febuary 4). *Sarbanes-Oxley (SOX) Act of 2002*. Retrieved from Investopedia: https://www.investopedia.com/terms/s/sarbanesoxleyact.asp

Livingstone, A., & Eliot, S. (2021, February 12). Disaster Recovery of Workloads on the AWS: Recovery in the Cloud AWS Whitepaper. Amazon Web Services Inc.

Mocan, T. (2019, February 20). *What is IKEv2.* Retrieved from Encryption Standards and VPN Protocols: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/

Shabe, C. (2017, May 10). *Understanding the App Develpoment Life Cycle*. Retrieved from DevOps.com: https://devops.com/understanding-app-development-life-cycle/

Sodabathina, R., & Rajamani, S. (2021). *Fine-tuning blue/green deployments on application load balancer.* Retrieved from AWS DevOps Blogs: https://aws.amazon.com/blogs/devops/blue-green-deployments-with-application-load-balancer/

Yubico Inc. (2021). *YubiKey 5 Series: The Multi-Protocol Security Key.* Palo Alto, CA: Yubico Inc.