SYSTEM CLIENT DESIGN

BRIAR MILLER
GERARD DOCTORA

TABLE OF CONTENTS

INTRODUCTION

New Zealand's Phone-Me company provides IP-phone services to customers nationwide. The Chief Technology Officer (CTO) has requested the design of a System Client to facilitate remote access, allow for updating of end-user personal information, and manage the services our end-users subscribe to. The CTO has emphasised that no end-user data should be stored locally on customer devices and that a two-phase security password protocol should be implemented. This report will cover regulatory requirements and analyse options to provide security and reliability for our customers and business. We will use our findings and considerations to support the proposed network infrastructure and practices.

BUSINESS OBLIGATIONS

Confidentiality, Integrity and Availability (CIA) are key principles in information security. In this design, we aim to ensure access and disclosure of the data and/or information is only to authorised personnel, while preserving its accuracy, completeness and accessibility when required. A method of achieving this would be incorporating the use of Amazon Web Services (AWS).

AWS cloud computing would allow Phone-Me to benefit from its wide range of services – including data storage, protection of sensitive information, access controls and mechanisms, and disaster recovery. AWS allows Phone-Me to increase scalability smoothly and without extra expenses. Options with the service can be customised to suit our needs as AWS continuously innovate and improve their technologies. Cloud-based computing allows expansion to all locations around the world, reducing latency [1] and improving customer experience.

DATA STORAGE

Data storage is crucial for all businesses as it ensures data preservation, business continuity, and seamless data accessibility. Reliable storage solutions also support compliance with legal and regulatory requirements. For Phone-Me's IP Phone service, scalable and efficient data storage is essential to accommodate growth and maintain operational efficiency. As the business evolves, our storage infrastructure must also adapt to support new technologies and future advancements.

In our design, we will utilise Amazon S3 (Simple Storage Service) for cloud-based storage. Amazon S3 supports high throughput and low latency for frequently accessed data, ensuring business continuity and seamless accessibility. It also supports data encryption at rest and integrates smoothly with AWS Key Management Service (KMS) for secure key management. Data being stored in S3 will be encrypted in transit and at rest to successfully safeguard Phone-Me and our customer's data

adhering to NIST standards. Additionally, Amazon S3 is a cost-effective solution, as Phone-Me only pays for the storage they use, offering scalability as the business expands. Overall, Amazon S3 is a reliable and flexible solution for storing, managing, and retrieving data in the cloud [1].

Amazon S3 will be used to store all passwords (hashed), sensitive data, and logs securely. To ensure that data is correctly classified, we will utilise Amazon Macie most importantly ensuring sensitive data is identified and protected appropriately. Our solution will satisfy our business obligation to prevent end-user data from being stored on customers' devices while securely protecting it.

DISASTER RECOVERY

Disaster Recovery (DR) is essential for our infrastructure to safeguard against data loss, ensure business continuity, maintain compliance, and protect Phone-Me's reputation. A comprehensive DR plan enables businesses to act quickly and minimise disruptions to operations. To achieve this, our design will leverage AWS Backup to rapidly restore operations and maintain access to Phone-Me's critical services and data during unexpected outages, failures or disasters. We will be using a cross-cloud strategy, directing and storing backups in another AWS account, ensuring if a breach, DDoS or ransom were to occur, Phone-Me is contingently covered. Regular data backups will be managed by AWS Backup, which automates backups across our entire build [2]. This service allows the creation of custom backup policies and schedules, ensuring data security while integrating seamlessly with AWS IAM for controlled access and monitoring and AWS KMS for data encryption on the isolated environment.

REGULATORY OBLIGATIONS

Phone-Me is obliged to adhere to legislation in place to protect customer's personal information. Due to Phone-Me being in New Zealand, but having the potential of foreign users within the country, it would be advised to simplify things with an initial disclaimer when new users first sign up to Phone-Me. This disclaimer could be signed when users first set up their IP Phone, and must initiate it by reading the disclaimer, and then putting in a unique code. The unique code would only be accessible to view from New Zealand. The following legislation would be the two that would protect Phone-Me users' personal data:

NEW ZEALAND PRIVACY ACT 2020

New Zealand's Privacy Act originated in 1993 to protect individual privacy by having more control over how personal data was collected, stored, and disclosed. The Act was then reviewed and rewritten in 2020, the key change being in the notification process of any privacy breaches a company may make

– transparency is a must. The Act was last updated 01 July 2024 and now has 13 key privacy principles, which together, "governs how organisations and businesses can collect, store, use and share your information" [3]. A breach of the Privacy Act 2020 in New Zealand can lead to a maximum fine of $10,000. Three of the principles will be covered, but more information for these can be found on legislation.govt.nz under Privacy Act 2020.

PRINCIPLE 4 – MANNER OF COLLECTION

Principle 4 centres around the way personal information is collected, it must be done in a fair and respectful manner. This principle ensures individuals are treated ethically, and no deception or coercive behaviour is involved when collecting data. Special care must be taken when it comes to anyone who are vulnerable, such as children, the elderly, or someone mentally impaired. Therefore, customer service and identification checks are the two most important themes here.

PRINCIPLE 5 – STORAGE AND SECURITY OF INFORMATION

Principle 5 focuses on the prevention of loss, misuse or disclosure of personal information through suitable forms of safeguards. Businesses are responsible for ensuring the correct steps are taken to fulfil this principle through physical security and cybersecurity measures. If a privacy breach were to occur, the level of this severity should be matched by the level of security put in place to stop this. Continuous reviews of security measures in place should occur, and changes should be made as necessary. Technology is forever advancing, along with the new risks businesses face. The final part of this principle focuses on reporting of breaches. If there is a breach, this must be disclosed as soon as possible and within 72 hours. There is an online form called NotifyUs [4] on the Privacy Commissioner's website for businesses to follow.

PRINCIPLE 13 – UNIQUE IDENTIFIERS

Principle 13 centres around organisations assigning unique identifiers to people when necessary for their functions, for example, a driver's licence number, passport number, IRD number, etc. Organisations are responsible for taking the correct steps to protect unique identifiers from misuse and make sure proper verification takes place when issuing them.

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is a law protecting data for residents of the European Union (EU). While New Zealand is not part of the EU, if New Zealand businesses deal with any EU residents' data, they must follow the GDPR. The GDPR is like the Privacy Act 2020, with some additions:

- A broad scope of countries is covered, whereas the Privacy Act covers only New Zealand,
- Individuals have the "Right to Erasure"; they can request to have their data deleted under some conditions,
- Individuals have the right to "Data Portability" – data can be shared across different services,
- A more regimented process for gaining consent,
- More details and requirements for specific roles, and
- A heftier fine. [5]

DATA INTEGRITY

Data integrity and authentication mechanisms are an important security requirement due to the sensitivity of dealing with personal information and data. Our Phone-Me design will use multiple techniques to add a layer of security. Data integrity ensures data remains original without being altered or tampered with. Three techniques to achieve this are using checksums, hashes, and digital signatures. Checksums create a unique value that travels with the content being sent to the receiver. When the content is opened at its intended destination, this value received is compared to the one sent originally. If these match, it indicates the content is untampered and unaltered. Hashes are similar to checksums but are much more complex and have stronger collision resistance.

HASHING

The Secure Hash Algorithm 256-bit (SHA-256) function is globally recommended and implemented by AWS KMS. SHA-256 is a cryptographic hash function that takes input data and processes it in blocks through mathematical operations. It produces a unique 256-bit hash value, making it nearly impossible to reverse-engineer or find two different inputs that generate the same hash so consequently it is collision and pre-image resistant. SHA-256 is slower than older and simpler algorithms like MD5 and SHA-1, but it is faster than other complex algorithms like SHA-3, being a good balance between maintaining data integrity and time. SHA-256 is compatible with most software and various applications and systems and has been proven to be robust for long-term use, whereas other algorithms are being phased out, like MD5 and SHA-1 [6]. SHA-256 is a trusted choice for securing transactions and data and can be used for digital signatures. Therefore, Phone-Me will use hashes through the Secure Hash Algorithm 256-bit (SHA-256) function.

SECURE CHANNEL COMMUNICATION

Data is highly vulnerable when in transit, making it a critical business responsibility to ensure its security during this phase. As data constantly moves across network infrastructures, it is essential to secure every path within the system. Protecting sensitive information in transit is not only a legal requirement but also aligns with standards like NIST, helping to prevent data breaches. Data in transit is susceptible to Man-in-the-Middle (MITM) attacks, where malicious actors can intercept, alter, or expose the data. From a business perspective, the integrity and security of data during transmission directly impact customer trust and the company's reputation.

In light of this, we have incorporated a couple of features into our design to ensure the security of sensitive information in transit. First, the connection between Phone-Me customers and the main AWS Cloud, will utilise Hypertext Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) encryption. Our AWS API Gateway associates with AWS Certificate Manager (ACM) to provision, manage, and deploy TLS certificates to our users providing a secure channel of communication. Our approach safeguards against Man-in-the-Middle (MITM) attacks by verifying the authenticity of the connection through handshakes and encryption, ensuring that data remains secure and unaltered during transit.

Another potential vulnerability lies in the communication paths between Phone-Me employees and both the main and backup AWS environments. These channels will be secured by first connecting to a Virtual Private Network (VPN) to access company resources, providing a secure and encrypted connection. Additionally, it allows employees to access the network remotely, even over unsecured public internet connections. Employees will launch their VPN client from devices such as laptops, desktops, or mobile phones, and authenticate via multi-factor authentication (MFA). Once logged in, the employee's device will be connected through a secure, encrypted tunnel to the Phone-Me network. During this process, the data exchanged remains private, and the VPN provider serves as an intermediary. This remote access setup provides the same level of security and functionality as a physical device within an office building.

AUTHENTICATION MECHANISMS

The primary purpose of an authentication mechanism is to verify proper authorisation before granting access. To achieve this, our design incorporates both password protection and multi-factor authentication (MFA). Password controls such as conditions and management will be structured against NIST standards.

PASSWORDS

Until recently, it was commonly thought the complexity of a password determined its security. However, after analyses of breached password databases conducted by NIST, it was revealed that complex passwords (usually including at least one number, uppercase letter, and symbol) negatively impacted usability and memorability without much benefit to security [7]. In accordance with NIST standards we will be focusing on password length, security controls and secure storage to protect against breaches. Our password management and conditions will involve the following:

- Password must not include commonly used words or phrases
- This will be screened against a database of 50,000 most common passwords e.g. *1234abcd, password1234, qwertyuiop*
- Password must be at least 12 characters in length, supporting up to 64 characters in length
- Password must not match a previously used password
- MFA is required in instances where a password has been successfully used
- SMS will not be used as an acceptable form of 2FA/MFA
- Passwords are considered sensitive data and thus encrypted using AES-256
- Passwords to be stored using:
    - SHA-256
    - 32-bit salting

MULTI-FACTOR AUTHENTICATION

Multi-Factor Authenticator (MFA). MFA refers to an authentication method that goes beyond usernames and passwords, such as biometrics, physical cards, emailed links or verification of a code through an application. Phone-Me will use Microsoft Mobile Phone Authenticator as its third-party MFA, which will serve as basic hygiene for our security posture. Biometric data is difficult to execute (however increasing threat of AI tools) - physical tokens can become expensive, and SMS confirmations are no longer considered acceptable according to NIST standards [7]. As our users will likely possess a smartphone, the application being implemented is Microsoft Authenticator as it is independent from AWS contributing to an extra layer or separation and security in an event AWS becomes compromised, and our tokens are intercepted.

MFA will confirm users attempting to access our system are who they say they are being prompted upon customer or internal user login, including during access to sensitive or protected resources. A user in Customer Services should not be able to access resources in Finance which MFA will facilitate authorisation and access to.

In conjunction with AWS IAM and MFA, Phone-Me will establish a conditional access policy where permissions will be granted on a need-to basis. It is essential to keep a good balance between useability and security to minimise the friction of providing high-quality service to our customers and productivity for our internal users.

ENCRYPTION AND KEY MANAGEMENT

Encryption and key management are fundamental to ensuring the confidentiality and integrity of sensitive data. Encryption protects data by transforming it into a format that is unreadable without the correct decryption key, preventing unauthorised access. Key management involves securely generating, storing, and distributing cryptographic keys used for this process.

The symmetric key management algorithm proposed in this application is AES-256 encryption. It will be used to safeguard critical information, providing a robust level of security that is nearly unbreakable. The secure management of cryptographic keys is vital to preventing data breaches, which is why AWS KMS (Key Management Service) is leveraged. AWS KMS offers centralised control over key creation, storage, and access, ensuring that keys are protected and used only by authorised systems and individuals. This service also simplifies compliance and monitoring, making it a vital part of Phone-Me's data security strategy.

AES-256

Encryption helps maintain the confidentiality of personal and private data, such as financial information and personal communications. AES-256 offers a good balance between security and performance.

AWS uses the Advanced Encryption Standard (AES) as a cryptographic algorithm to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt digital information. It can use cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [8]. Its purpose will be to comprehensively obfuscate information in transit to and at rest in our AWS S3 buckets, acting as an additional layer of protection from unauthorised personnel, especially in the event of a security breach. AES-256 is an industry-trusted algorithm commonly used by large organisations globally, including the U.S. Government [9] due to its resilience against brute-force

attacks. While no encryption standard is absolutely secure, AES-256 is the best option to protect Phone-Me's sensitive information. AES-256 is used globally and supported by most modern encryption libraries, so implementation should be seamless, additionally complying with NIST and GDPR.

Other options for symmetric key management algorithms are 2DES and 3DES [10], which we did not opt for use due to the following:

- 2DES
    - Key size limitations: typically use 112-bit keys, however with this key size the algorithm is known and does not provide sufficient security against modern computational power.
    - Performance Issues: slower than many modern encryption algorithms, such as AES. The double application of standard DES adds computational strain without significantly enhancing the security
    - Meet-in-the-Middle Attacks: susceptible to meet-in-the-middle attacks, which significantly reduces the security and privacy of the connection.

- 3DES
    - Compatibility Issues: 3DES is an outdated symmetric key algorithm, and integrating 3DES into modern systems can lead to compatibility issues. With the advancement of technology and newer encryption algorithms we would have to change our infrastructure catering to 3DES, which would be counterintuitive to futureproofing our systems.
    - Performance Issues: significantly slower to AES as it applied standard DES three times. The triple encryption process introduces additional computational strain, which can be a disadvantage in performance-critical applications.
    - Key size limitations: While there is no known exploit against 3DES, it is still inferior, with a limit of 168-bit keys versus 512-bit keys for AES.

KEY DISTRIBUTION

Key distribution methods are essential for the secure management of cryptographic keys, which play a critical role in protecting sensitive data. Effective key distribution ensures that encryption keys are shared and managed securely among authorised users and systems, preventing unauthorised access and potential data breaches. The design involved the use of AWS KMS, a fully managed service that simplifies the creation, management, and control of cryptographic keys used to encrypt data. It provides a centralised platform for managing customer master keys (CMKs), ensuring that keys are securely generated, stored, and accessed. These CMKs can be either symmetric for encrypting data

and asymmetric for verification or digital signing purposes. This service integrates seamlessly with various AWS services, enabling automatic encryption and decryption of data without requiring our customers to handle keys directly. Whenever a customer is kept from handling a key directly it reduces the likelihood of any key compromise as no exchange is being performed, ultimately increasing the security of our data and information [11].

AWS KMS provides phone-me with the following functionalities:

- Centralised Control: AWS KMS acts as a central repository for creating, managing, and storing CMKs.
- Key Policies and Access Control: Phone-me can define key policies that specify who can use or manage the keys. In conjunction with our access controls, we can configure authorisation using AWS Identity and Access Management (IAM) roles and policies.
- Automatic Key Generation and Distribution: When a key is needed for encryption or decryption, KMS automatically generates and distributes data encryption keys. These keys are generated on-demand and used to encrypt data while the CMK remains secure within KMS.
- Secure Key Storage: Keys are stored within AWS infrastructure, ensuring that they are not exposed to unauthorised access.
- Audit and Compliance: AWS KMS integrates with AWS CloudWatch to log key usage, providing an audit trail for compliance and monitoring purposes.

If Phone-me were to manage our own key distribution and storage, the best option is a Public Key Infrastructure (PKI), which uses symmetric key algorithms to encrypt the data and asymmetric algorithms to distribute the private key securely (as a public key). After fulfilling the certificate request, authority and acquisition, our customers can securely transfer data this way. A reason for not opting to go in this direction is it would require more operational overhead, allowing the team to focus on application development versus key maintenance. Scalability is also a major concern as AWS KMS negates additional infrastructure requirements necessary to facilitate PKI. We would also lose out on capabilities such as logging and integration with other AWS tools.

ACCESS CONTROL MANAGEMENT AND MODELS

Access control is the cornerstone of cybersecurity. It allows businesses to control and regulate those who have access to data, applications, or systems. Access control enables the safekeeping of sensitive data and ensures operational integrity.

ACCESS CONTROL MANAGEMENT

Managing access to our infrastructure is a critical component of security. Phone-Me has a responsibility to protect sensitive data, mitigate security risks, maintain operational integrity, and ensure compliance, all of which work together to minimise the risk of data breaches and tampering. Different individuals will need varying levels of access based on their roles. To achieve this, access to throughout our infrastructure will be managed through AWS IAM (Identity and Access Management). AWS IAM allows for the control of who can access specific resources and what actions they are authorised to perform. With IAM, we can create and manage individual users, groups, and roles, providing tailored access to meet the needs of each user. For added security, IAM supports Multi-Factor Authentication (MFA), specifically MS Authenticator, particularly for user login or users accessing sensitive resources. AWS IAM also allows temporary access when necessary, providing flexibility as Phone-Me scales. Importantly, AWS IAM's pricing model ensures that Phone-Me only pays for what it uses, keeping it cost-effective as the business grows [12].

ROLE BASED ACCESS CONTROL (RBAC)

RBAC focuses on the user's role rather than the user's identity, it is based on Users-to-Roles. These roles can come under job profile, responsibility, and authority within the organisation. The RBAC has a matrix to provide straightforward management of each role. When adding, editing, or deleting a role or individual employee into the system, this matrix can be referred to for direction (Appendix 1). RBAC also consists of four models that relate to each other, visually available in Appendix 1. The models are RBAC 0, which contains the minimum functionality; RBAC 1, which contains role hierarchy along with RBAC 0; RBAC 2, which contains constraints along with RBAC 0 functionality; and RBAC 3, which is the consolidated model containing functionalities of all three models. Some constraints could include geolocation; if an employee logs in overseas, the model will restrict access. If an employee gets their password incorrectly more than three times in a row, the account will be locked. RBAC has three primary rules: role assignment, role authorisation, and permission authorisation. Some advantages of RBAC include flexibility, ease of maintenance, centralised, non-discretionary policies, and lower risk exposure. However, using RBAC can be a complex deployment, balancing security with simplicity can be difficult, and layered roles and permissions can increase risk.

DISCRETIONARY ACCESS CONTROL

DAC involves the resource owner defining the users' access control policy. Therefore, the owner controls who can read, write, execute, search, create, and delete. DAC is commonly also known as the Need-to-Know access model and is based on Users-to-Subjects. DAC manages control via user identification with supplied credentials during authentication, such as username and password. File access permissions are stored in an access control matrix, a database that maintains which users can access what resources and what they can do with them. The access control matrix rows are used to denote the users/subjects, the columns denote the objects/resources, and the values denote the access permissions that have been assigned (Figure 1). The advantages of the DAC model are that it is conceptually simple and can be responsible for business needs. However, it can over or under-privileged users, there is limited control, and security can be compromised by human error and missing oversight.

ACCESS CONTROL APPLICATION

Based on Phone-Me's needs, RBAC would be most suitable. Phone-Me is a growing business, and it will not stay small for long, so RBAC is better in the long term. Therefore, managing permission based on roles will be easier to manage rather than on an individual basis. Phone-Me will have a structured hierarchy, which means it will be easier to assign a user to a role. For security, there is less risk with RBAC due to enforcing the “least privilege” principle, meaning the risk of unauthorised access is minimised. Phone-Me will deal with sensitive data daily, so this lowered risk is necessary. Although DAC allows for more flexibility and a more creative environment with less structure, DAC can lead to complexities and inconsistencies in access. Permissions are set by the users and not central rules. This can create a messy management of sensitive data. There is more risk of accidental over-privileged users in a larger organisation; things get overlooked. In DAC would be best for a smaller and more flexible organisation.

NETWORKING SECURITY

Networking security is essential for protecting cloud-based applications and infrastructure from threats while ensuring data confidentiality, integrity, and availability. Key components of networking security include AWS Web Application Firewall (WAF) for filtering and blocking malicious traffic, AWS CloudWatch for monitoring network activity and providing real-time logging and alerts, and network segmentation to isolate critical systems and reduce the risk of widespread compromise.

WEB APPLICATION FIREWALL (WAF)

A Web Application Firewall (WAF) and infrastructure monitoring are essential for protecting and maintaining the security and performance of web applications and services. AWS WAF helps defend against common web threats by filtering malicious traffic before it reaches the application [13]. AWS WAF allows protection through the creation of custom rules like blocking requests from certain IP addresses, geographies, or those with specific header values. Distributed Denial-of-Service (DDoS) attacks are also mitigated through rate-limiting, controlling the number of requests a single user can make to our services.

INFRASTRUCTURE MONITORING

Infrastructure monitoring with AWS CloudWatch provides real-time alerts [14] of security issues and system logging, allowing to identify and address issues before they impact the service, ensuring availability and reliability for users. Real-time monitoring means we can respond to threats or issues rapidly mitigating damage from occurring or growing, while logging [15] provides threat-hunting and auditing/investigation capabilities.

NETWORK SEGMENTATION

Network segmentation is a critical practice for enhancing security and controlling traffic flow within a cloud environment. It is especially important in this design as the public subnet is used to host the API, making it accessible to external users over the internet, while private subnets are used to host sensitive backend services and databases that should not be directly accessible from outside. This segmentation ensures that only the API in the public subnet is exposed to external traffic, while the private subnet is shielded from direct access, reducing the attack surface. By placing the customer-facing components in the public subnet and isolating the internal resources in private subnets, we can better enforce access controls, monitor traffic, and protect sensitive data, maintaining a secure boundary between public-facing and internal network resources.

CONCLUSION

In conclusion, the proposed System Client design effectively meets the CTO's requirements and ensures compliance with relevant regulations, including the New Zealand Privacy Act 2020 and the GDPR, which govern the protection of sensitive data. The cloud-based design, hosted on AWS, supports remote access, while updates to personal information or service subscriptions are managed securely through an API-accessible web application. No data is stored on end-user devices; instead, it is safeguarded within Phone-Me's private subnet. To enhance security, the design includes a two-phase password protocol using Microsoft Authenticator alongside AES-256 encryption, SHA-256 hashing, and secure digital signatures in alignment with NIST standards. Secure key distribution is managed through AWS KMS within a VPC, and access control is enforced via the RBAC model and AWS IAM.

This design keeps our internal network isolated from external users and traffic. In conjunction with proper security practices and mechanisms, we can provide strong resistance against breaches and widespread damage. Consequently, this increases our reaction window as we monitor our infrastructure using AWS CloudWatch. Overall, this solution confidently addresses the CTO's requirements while adding robust security and regulatory compliance measures.

REFERENCES

[1] Amazon Web Services, “Amazon S3,” [Online]. Available: https://aws.amazon.com/s3/.

[2] AWS, “AWS Backup,” [Online]. Available: https://aws.amazon.com/backup/.

[3] Privacy Commissioner, “Privacy Act 2020 and the Privacy Principles,” [Online]. Available: https://www.privacy.org.nz/privacy-act-2020/privacy-principles/.

[4] Privacy Commisioner, “NotifyUs - For organisation to report privacy breaches,” [Online]. Available: https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us.

[5] GDPR, “General Data Protection Regulation,” 2024. [Online]. Available: https://gdpr.eu/tag/gdpr/.

[6] F. Mendel, N. Pramstaller, C. Rechberger and V. Rijmen, “Analysis of step-reduced SHA-256,” in *Fast Software Encryption: 13th International Workshop*, Graz, Springer Berlin Heidelberg, 2006, pp. 126-143.

[7] National Institute of Standards and Technology (NIST), “Digital Identity Guidelines,” 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[8] Federal Information Processing Standards Publication, “Advanced Ecryption Standard (AES),” May 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

[9] Arcserve, “5 Common Encryption Algorithms and the Unbreakables of the Future,” September 2023. [Online]. Available: https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future.

[10] Coded Insights, “Double DES and Triple DES,” [Online]. Available: https://codedinsights.com/modern-cryptography/double-des-and-triple-des/.

[11] AWS, “AWS Key Management Service,” [Online]. Available: https://aws.amazon.com/kms/.

[12] AWS, “AWS Identity and Access Management,” [Online]. Available: https://aws.amazon.com/iam/.

[13] Amazon, “AWS WAF,” n.d.. [Online]. Available: https://aws.amazon.com/waf/.

[14] Amazon, “Application Monitoring,” n.d.. [Online]. Available: https://aws.amazon.com/cloudwatch/features/application-monitoring/.

[15] Amazon, “What is Amazon CloudWatch Logs?,” n.d.. [Online]. Available: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html.

[16] S. Apte, D. Bokefode, G. Modani and A. Ubale, “Analysis of DAC MAC RBAC Access Control based Models for Security,” *International Journal of Computer Applications (0975 – 8887),* vol. 104, no. 5, p. 13, 2014.

APPENDIX

FIGURE 1 - CLIENT-SERVER PLATFORM DESIGN

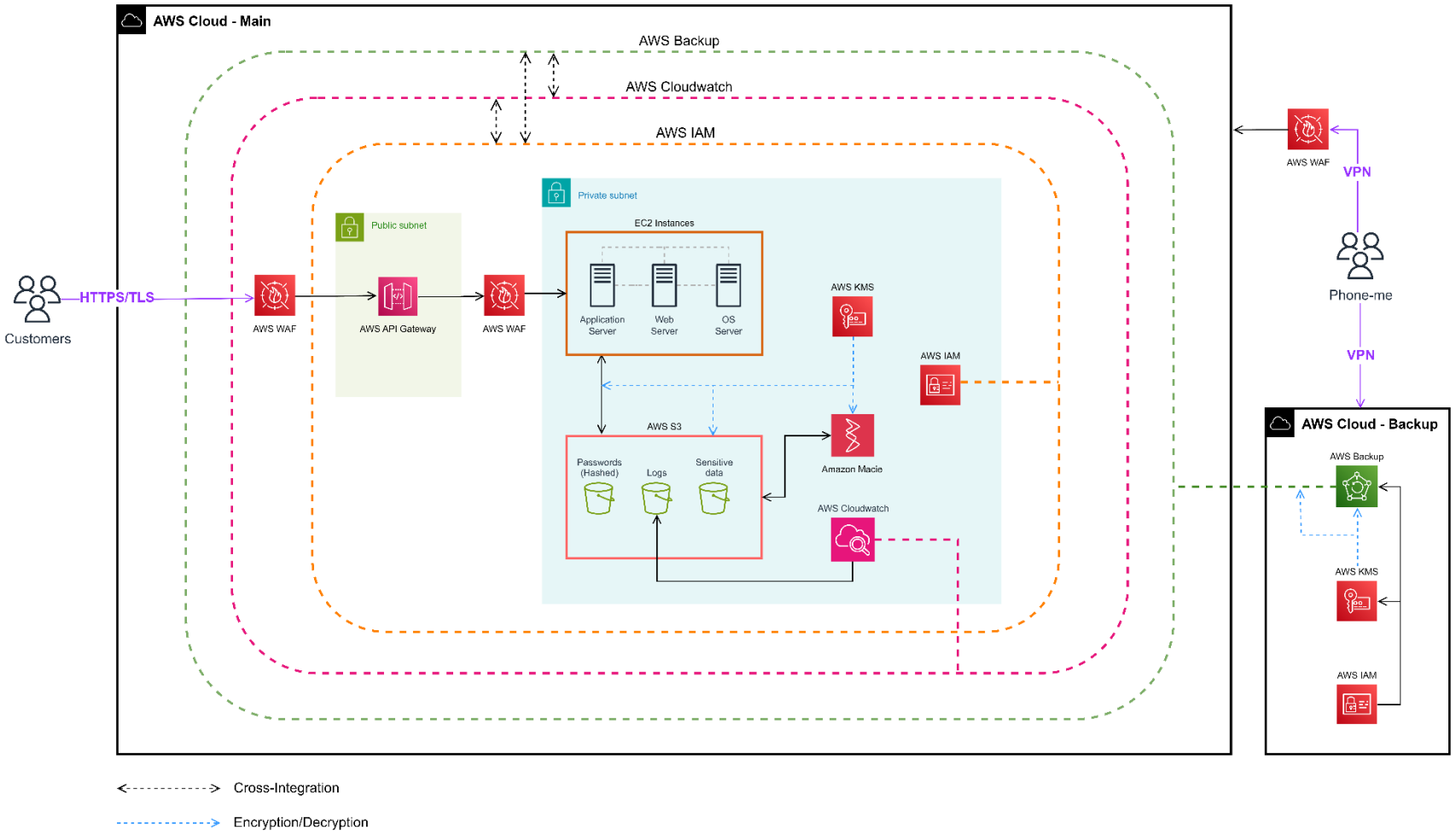
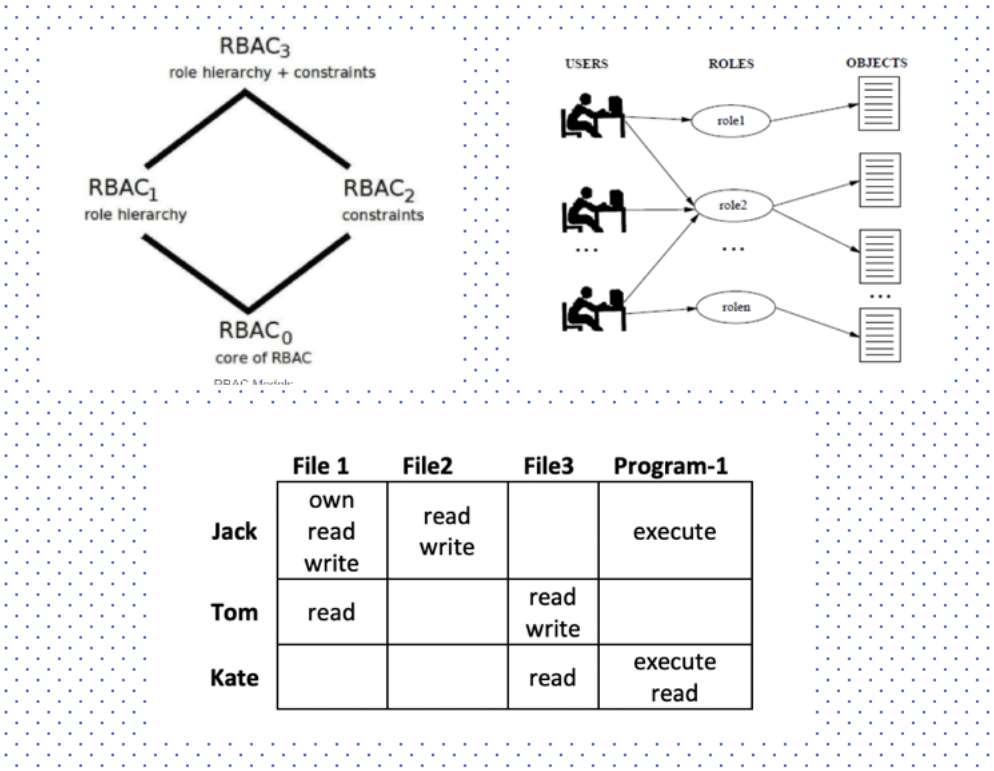


FIGURE 2 – ANALYSIS OF DAC RBAC ACCESS CONTROL BASED MODELS FOR SECURITY



	File 1	File2	File3	Program-1
Jack	own read write	read write		execute
Tom	read		read write	
Kate			read	execute read

[16]