Project Report

by:

Syed - 301318212

for:
CBER 703 – Cyber Forensics

Centennial College

School of Engineering Technology and Applied Science

to:

Dr. Atiqur Rahman
on:

Date: April 2nd, 2024.

Table of Contents

Cloud Encryption

In the era of digital transformation, cloud computing has become fundamental, revolutionizing data and application storage, access, and processing for businesses. The cloud's agility, scalability, and cost-effectiveness have made it popular for optimizing IT infrastructure and fostering innovation. However, this convenience brings the critical responsibility of ensuring data security and protecting sensitive information. Data encryption plays a crucial role in this, serving as a robust defense mechanism to safeguard data confidentiality and integrity in cloud environments. Encryption transforms plain text data into ciphertext, guaranteeing that only authorized individuals possessing the correct decryption keys can retrieve the information. With organizations relying on cloud providers for their data, robust encryption techniques and key management strategies are essential to instill trust and confidence in cloud services.

Importance of Encryption

Encryption is a fundamental aspect of a defense-in-depth security strategy, providing an additional layer of protection beyond access control. It works by converting data into unreadable ciphertext using algorithms and keys, ensuring that only authorized parties can access the original data. Strong encryption algorithms like AES-256 make it computationally infeasible to decrypt data without the correct key, offering robust data security.

In a security strategy, encryption complements access control mechanisms by mitigating potential weaknesses. Even if access controls fail, encrypted data remains protected, preventing unauthorized access. AWS, for example, utilizes AES-256 encryption for services like Amazon S3, ensuring data security even in the event of a breach.

Key requirements for an effective encryption solution include protecting keys at rest and ensuring independent key management. Systems must secure encryption keys to prevent unauthorized usage and implement encryption algorithms correctly. Independent key management ensures that access to encryption is separate from data access control, enhancing security.

Cryptography in Cloud

Cryptography is a method used to safeguard information by converting it into an unintelligible form, with a primary goal of ensuring confidentiality, particularly in cloud settings. There are two primary categories of algorithms employed for cryptographic purposes in the cloud: symmetric and asymmetric. Symmetric encryption is favored for its rapidity and effectiveness, especially in scenarios involving extensive data storage. It relies on a single shared key for both encrypting and decrypting data, ensuring secure communication among users. The Data Encryption Standard

(DES) is a widely utilized symmetric encryption algorithm that works on fixed-size blocks of plaintext information.

Asymmetric encryption, in contrast, utilizes a pair of distinct keys: a public key for encryption and a private key for decryption. Despite offering heightened security, asymmetric encryption is slower and demands more resources than symmetric encryption. Public keys are openly shared and utilized for encryption and verification, whereas private keys are kept confidential and employed for decryption purposes.

Cloud cryptography algorithms are designed to ensure data safety and reduce the risk of cyberattacks by creating efficient and secure encryption methods. These algorithms depend on three main dimensions:

1. Type of Operation:
   - Substitution: Mapping each plaintext element to elements in the ciphertext.
   - Transposition: Rearranging plaintext elements for encryption.

2. Number of Keys:
   - Algorithms are classified into symmetric and asymmetric models based on the number of keys involved.

3. Plaintext Processing”
   - Block cipher: Creating an output block for each input, encrypting each block.
   - Stream cipher: Continuously encrypting input elements, producing output one element at a time.

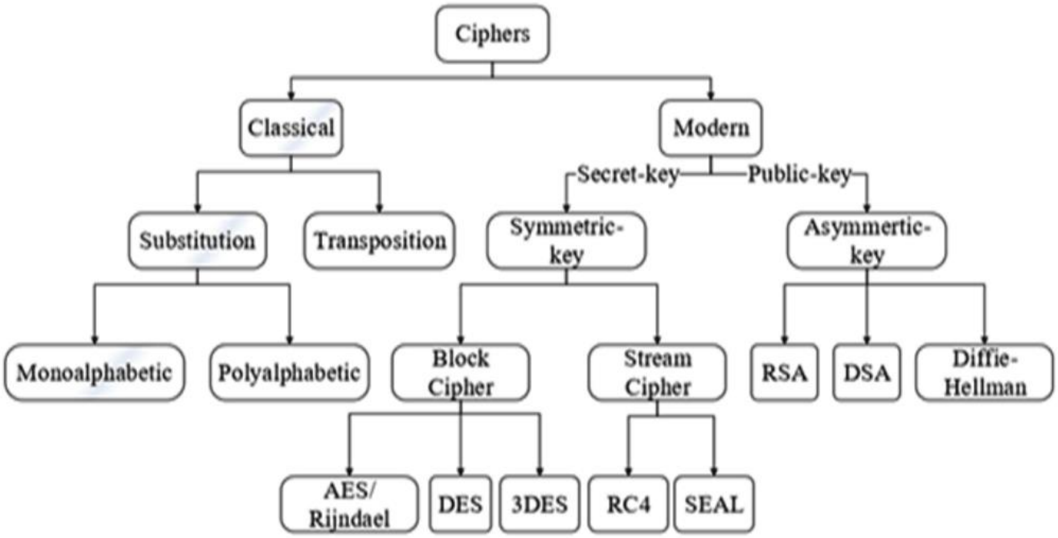

Figure 1 - Classification of Encryption Algorithms

Cryptography in cloud computing architecture often requires physical hardware modules for security and segregates key management and cryptographic operations within a secure crypto-domain. This architecture ensures the protection of keys and cryptographic operations from unauthorized access, enhancing overall data security in cloud environments.

Key challenges in cloud data encryption:

1. Managing encryption keys at scale.
2. Addressing performance overhead of advanced encryption techniques.
3. Balancing security with usability.

Future research areas:

1. Improving homomorphic encryption efficiency.
2. Exploring post-quantum encryption.
3. Developing automated key management solutions.

Cloud Service Providers and Offerings

Amazon Web Services (AWS) is the leading cloud computing platform, offering over 200 services catering to individuals, enterprises, and governments. It originated as an internal cloud service for Amazon.com and became publicly available in 2006 with services like Amazon S3 and EC2.

Microsoft Azure, launched in 2010, is the second-largest cloud platform, boasting over 200 products and services. It caters particularly to Microsoft-centric enterprises, supporting both Windows-based and open-source technologies, and is widely used by Fortune 500 companies.

Google Cloud Platform (GCP), part of the broader Google Cloud offering, was introduced in 2010. With over 100 services, GCP provides computing, networking, and big data solutions. It includes services like Google Workspace and supports enterprise Android and Chrome OS.

Table 1 - Comparison of Cloud Services

Category	AWS	Azure	GCP
Infrastructure as a Service (IaaS)			
Compute Services	EC2 (Elastic Compute Cloud)	Virtual Machines	Compute Engine
	AWS Lambda	Azure Functions	Cloud Functions
Storage Services	S3 (Simple Storage Service)	Blob Storage	Cloud Storage

	EBS (Elastic Block Store)	Managed Disks	Persistent Disk
	Glacier	Blob Storage (Cold Tier)	Cloud Storage Nearline/Coldline
	EFS (Elastic File System)	File Storage	Filestore
Networking	VPC (Virtual Private Cloud)	Virtual Network	Virtual Private Cloud (VPC)
	Direct Connect	ExpressRoute	Cloud Interconnect
	Route 53	Azure DNS	Cloud DNS
Identity & Access	IAM (Identity and Access Management)	Azure Active Directory	Cloud IAM
Platform as a Service (PaaS)			
Compute Services	Elastic Beanstalk	App Service	App Engine
	ECS (Elastic Container Service)	Kubernetes Service (AKS)	Kubernetes Engine
	Fargate	Azure Container Instances	Cloud Run
Database Services	RDS	SQL Database	Cloud SQL
	ElastiCache	Cache	Memorystore
	Neptune	Cosmos DB	Firestore
	DocumentDB	Table Storage	
	Redshift	Synapse Analytics	BigQuery
Serverless Computing	Lambda	Azure Functions	Cloud Functions
	Step Functions	Logic Apps	
Software as a Service (SaaS)			
Email & Productivity	WorkMail	Office 365	Google Workspace (G Suite)
	WorkDocs	Outlook	Gmail
		OneDrive	Drive
Collaboration	Chime	Teams	Hangouts, Meet
Customer Relationship Management	Connect	Dynamics 365	CRM
Business Intelligence	QuickSight	Power BI	Data Studio

Forensics Software Validation Procedure

1. Objective:
The objective of this procedure is to establish a systematic approach for validating new forensics software packages within our organization. This process ensures that selected software meets the necessary criteria for reliability, accuracy, compatibility, and adherence to industry standards.

2. Scope:
This procedure applies to all new forensics software packages considered for integration into our lab environment.

3. Responsibilities:

- **Forensics Software Validation Team:** Responsible for executing the validation process outlined in this procedure.
- **IT Department:** Provides support for setting up testing environments and ensures compatibility with existing infrastructure.
- **Vendor Relations:** Engages with software vendors to obtain necessary information and trial versions.

4. Validation Procedure:

4.1. Define Validation Criteria:

- Criteria include functionality, reliability, accuracy, compatibility, and adherence to industry standards such as ISO/IEC 27037.

4.2. Research and Selection:

- Research potential forensics software packages based on defined criteria.
- Consult trusted sources such as NIST's Computer Forensics Tool Testing program.

4.3. Vendor Communication:

- Engage with software vendors to gather detailed information and obtain trial versions or demo licenses.

4.4. Testing Environment Setup:

- Set up a controlled testing environment mirroring production environment specifications.
- Implement safeguards to protect sensitive data and maintain testing integrity.

4.5. Functional Testing:

- Conduct functional testing to evaluate software capabilities against defined criteria.
- Test features including data acquisition, analysis, reporting, and integrity checking.

4.6. Performance Testing:

- Assess software performance under varying workloads and conditions.
- Measure processing speed, resource utilization, and scalability.

4.7. Compatibility Testing:

- Test software compatibility with different operating systems, file systems, and hardware configurations.
- Ensure integration with existing forensic tools and workflows.

4.8. Validation Documentation:

- Document test results, observations, issues, and resolutions.
- Prepare detailed reports outlining software strengths, weaknesses, and suitability.

4.9. Peer Review:

- Solicit feedback from experienced forensic analysts and IT professionals within the organization.
- Incorporate feedback into the evaluation process as appropriate.

4.10. Final Decision:

- Based on testing results and peer feedback, make an informed decision regarding software adoption.
- Consider factors such as cost, support options, and long-term viability.

5. Documentation:

- Maintain records of all validation activities, including test plans, reports, and decision memos.

6. Review and Update:

- Periodically this procedure will reflect to changes in technology, standards, or organizational needs.

7. References:

- ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.
- NIST Computer Forensics Tool Testing (CFTT) Program.

8. Approval:

- This procedure is approved by Syed (CISO).
- Approval Date: April 1st, 2024.

9. Distribution:

- This procedure is distributed to all relevant personnel involved in forensics software validation.

10. Revision History:

- Document any revisions made to this procedure, including dates and reasons for changes.

References

Abbas, F., & Khan, K. (2023, July). (PDF) cloud security: To prevent unauthorized access using an ... https://www.researchgate.net/publication/332662668_Cloud_security_to_prevent_unauthorized_access_using_an_efficient_key_management_authentication_algorithm

Beer, K. (2020, June 11). The importance of encryption and how AWS can help | amazon web ... https://aws.amazon.com/blogs/security/importance-of-encryption-and-how-aws-can-help/

Cloud computing services - amazon web services (AWS). (n.d.). https://aws.amazon.com/

Cloud computing services: Microsoft Azure. Cloud Computing Services | Microsoft Azure. (n.d.). https://azure.microsoft.com/en-us

Computer Forensics Tool Testing Program (CFTT). NIST. (2019, November 16). https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt

GfG. (2023, December 11). *Validating and testing forensics software*. GeeksforGeeks. https://www.geeksforgeeks.org/validating-and-testing-forensics-software/

Google. (n.d.). Google. https://cloud.google.com/

ISO. (n.d.). https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

Kent, K., Chevalier, S., Grance, T., & Dang , H. (2006, August). NIST SP 800-86, guide to integrating forensic techniques ... https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf

Sindhu, K. K. (2012, January). (PDF) Digital Forensics and Cyber Crime Datamining. https://www.researchgate.net/publication/272668132_Digital_Forensics_and_Cyber_Crime_Datamining

Wickramasinghe, S. (2021, October 1). *AWS vs azure vs GCP: Comparing the big 3 cloud platforms*. BMC Blogs. https://www.bmc.com/blogs/aws-vs-azure-vs-google-cloud-platforms/