How Cryptography Can Augment Zero Trust

Samuel Aiello
Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota, 57042, USA.

Email: sam.aiello@trojans.dsu.edu (S.A.)
Manuscript received September 12, 2023; accepted September 21, 2023; published September 25, 2023.
DOI: 10.18178/IJBTA.2023.1.1.52-60

Abstract: The scope of this work presents the security architecture of the Cloud provider/consumer and showcases how "Cryptography" augments the Zero Trust Architecture security strategy. In addition, this work will delve into enforcing the minimum expected set of security controls that assures secure isolation, data protection, access control and monitoring/logging at all tiers of the hosted applications. Cryptographic solutions play an important role in the cloud environment in which customers hand over data to a cloud provider for storage, and processing. One of the biggest hurdles for the adoption of cloud computing by enterprises is security and confidentiality. The premise of the paper will be that the cloud provider acts as a distrusted black box from the client's perspective, and whose duty and interest is the protection of their information and privacy. The techniques presented are shared jointly between the service provider and client, and should protect the interests of both, in establishing a successful and trustworthy service.

Keywords: Encryption, cryptography, PKI, single sign-on, multifactor authentication, authentication, authorization

1. Introduction

"Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud [1]. It allows users too conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange." There are three areas of data exposure: data in transit, data at rest, and data in use.

1.1. Business and Cloud Benefits Examined

Cryptography addresses four distinct problems. The first being confidentiality whereby we can protect who can see a message. The second issue that's addressed by crypto is data integrity where we can assure that data has not been tampered with. The third issue is authentication whereby we can confirm that a message is authentic and has not been forged. The fourth issue that's addressed by crypto is non-repudiation whereby we can verify the owner or the sender of a message, in fact, did originate that data.

1.2. Cloud Planning and Strategy- Encryption & Key Control

Encryption is currently available for data in transit and for data at rest. Data in Use is data in memory or being processed by hardware [2]. Where shared hardware is in use, data in use requires consumers must evaluate the Cloud Service Providers (CSP) isolation controls. If isolation controls aren't sufficient, dedicated resources may be the only resolution.

Key control allows consumers to protect data by encryption in instances where it retains the encryption keys. Whether the CSP uses their own layers of encryption, consumers should use encryption where the keys are retained by themselves and not the CSP whenever encryption is required. This mitigates the risk of

accidental or intentional decryption of data by parties other than the consumer.

2. Solution Implementation

2.1. Security Use Cases

An identity system must meet many conditions [3]. The use cases for identity management are:

1) Login/Logout- User log in/ log out to a system, an application, or other controlled access context.
2) Single Sign On- user logs in to one system, application, and so on and is thereby granted access to other related systems.
3) Multifactor Authentication- (MFA), users are required to provide more than one form of verification before gaining access to their accounts or systems. When used in conjunction with a user name and password, it provides an additional safeguard to access to systems and data.
4) Password and Identity Information Synchronization- When a password or other user identity information is changed, it is synchronized throughout the identity realm.
5) Add/Delete User Identity- information is added or deleted for a user throughout the identity realm.
6) Authentication- The identity system verifies a user's identity.
7) Authorization- The identity system verifies that the authenticated subject has specific permissions to perform an operation or access a specific resource.
8) Audit and Reporting- The logging of security relevant events related to any identity operation.

2.2. Security Requirements and Compliance

Cloud computing introduces unique security challenges because cloud operators store and handle consumer data outside of the control of the clients' existing security environment [4]. Practices of the CSP may be more or less stringent then the clients', but still have to be investigated before entering into an agreement with the CSP who would in turn then provides the appropriate security control on behalf of the client.

2.2.1. Cryptographic requirements

A PKI is a combination of software and procedures providing a means for managing keys and certificates, and using them efficiently [5]. Just recall the complexity of the operations described earlier in this article for having a feel on the absolute necessity to provide users with appropriate software support for encryption and digital signature. But nothing has been said yet about management.

Key and certificate management is the set of operations required to create and maintain keys and certificates. The following discussion outlines the major points being addressed in a managed PKI. A PKI must offer software support for key pair generation as well as certificate requests. In addition, procedures must be put in place to verify the user identity prior to allowing him to request a certificate.

Certificates are widely accessible because they are used for either encryption or signature verification. Private-keys require a reasonable level of protection because they are used either for decryption or for digital signature. A strong password mechanism must be part of the features of an effective PKI.

A PKI must provide a means by which a certificate can be revoked. Once revoked, this certificate must be included in a revocation list that is available to all users. A mechanism must be provided to verify that revocation list and refuse to use a revoked certificate. Without key backup, all messages and files that have been encrypted with his public-key can no longer be decrypted and are lost forever. A PKI must offer private-key backup and a private-key recovery mechanism such that the user can get back his private-key to be able to get access to his files.

2.3. Building Blocks

Utilizing encryption, data is scrambled or obfuscated. A key is used to encrypt plaintext to result in an encrypted value or ciphered text [3]. Decryption can only occur with the matching key to reveal the original message. Data in transit and at rest is stored in this encrypted format.

Hashing takes the data, puts it through an algorithm, and produces a result that is a unique value called a hash. Before using the encrypted data, another hash can be re-computed and if the hash value on data is the same as the as the original then it validates data authenticity. If the value is different, it means that the original data has changed. To get back to the original message, the decryption process is performed in reverse on the ciphered text.

2.4. Security Architecture

In the cloud, application security must include end-to-end security as part of the application design. This applies to both internal end-to-end communications as well to Internet end-to-end communications [5]. Data in-transit protection is provided by Transport Layer Security (TLS), or Secure Sockets Layer (SSL), or IP Security (IPsec).

2.4.1. Transport Layer Security (TLS)

Transport Layer Security is a TCP/IP session layer protocol. TLS gets used instead of the earlier SSL protocols [5]. It supersedes SSL. It provides a communication security framework over a computer network. The TLS process utilizes PKI certificates along with cryptography to establish trust between communicating entities. Both entities must negotiate a session encryption key as well as a cipher, which is used to protect the data communication between the parties.

The TLS deployment is supported by public key infrastructure (PKI) [5]. This is a hierarchy of digital certificates that contain public and private keys that are used to secure data. Certificate authorities, or CAs, also play a large role. The certificate authority is at the top of the PKI hierarchy. It is a trusted third party that is trusted by a certificate owner as well as by the party that relies upon the trustworthiness of the certificate. So the CA then issues PKI certificates.

TLS encapsulates and encrypts data transmissions via application-specific protocols such as HTTP, FTP, and SMTP. If there's a number of different web and mail servers that use HTTP and SMTP, TLS has to be configured for each.

2.4.2. Secure Sockets Layer (SSL)

Secure Sockets Layer or SSL predates TLS [5]. It is a TCP/IP model session layer protocol. SSL provides communication security over a computer network. But the final version of SSL was 3.0. SSL is now deprecated, and TLS has taken its place.

2.4.3. IPsec

IPsec is a TCP/IP network layer protocol. It gets deployed to secure Internet Protocol communications. IPsec can protect all application traffic over an IP network [5]. Unlike TLS or SSL, it doesn't require having to configure it per application. With IPsec, IP packets are authenticated and encrypted after negotiation between end point entities that want to communicate with one another.

It has several message protection modes which could be between a pair of hosts, host-to-host, between a pair of security gateways, network-to-network, which might be used, for example, as an IPsec VPN, or between the security gateway and a host, network-to-host. IPsec offers support for network-level peer authentication.

When examining a standard unencrypted datagram, the IP header followed by the IP payload are exposed. In transport mode with IPsec, instead following after the IP header, is an ESP header (Encapsulating Security Payload) for confidentiality. Even if someone were to capture this traffic on a network, not only would the actual payload be encrypted but they wouldn't even know what type of traffic it is.

3. Security Architectural Characteristics for Identity Protection

Cloud data protection characteristics parallel protecting data within a traditional data center.

3.1. Guidance for Security and Compliance—Authentication and Identity

"Maintaining confidentiality, integrity, and availability for data security is a function of the correct application and configuration of familiar network, system, and application security mechanisms at various levels in the cloud infrastructure. Among these mechanisms are a broad range of components that implement authentication and access control. Authentication of users and even of communicating systems is performed by various means, but underlying each of these is cryptography. Authentication of users takes several forms, but all are based on a combination of authentication factors: something an individual knows (such as a password), something they possess (such as a security token), or some measurable quality that is intrinsic to them (such as a fingerprint). Single factor authentication is based on only one authentication factor. Stronger authentication requires additional factors; for instance, two factor authentication is based on two authentication factors (such as a pin and a fingerprint) [3]"

"Authentication is usually predicated on an underlying identity infrastructure. The most basic scheme is where account information for one or a small number of users is kept in flat files that are used to verify identity and passwords, but this scheme does not scale to more than a very few systems. A full discussion of identity and access controls is beyond the scope of this book, but the key to effective access controls is the centralization of identity [3]"

3.1.1. Access control techniques

Access control mechanisms are a key means by which we maintain a complex IT environment that reliably supports separation and integrity of different levels or categories of information belonging to multiple parties. But access controls do not stand on their own; they are supported by many other security capabilities.

When discussing access controls, subjects and objects refer to people or processes acting on their behalf and files or other resources (a directory, device, or service of some sort)

3.1.2. Common types of access controls

Discretionary Access Control (DAC) In a system, every object has an owner [5]. With DAC, access control is determined by the owner of the object who decides who will have access and what privileges they will have. Permission management in DAC can be very difficult to maintain; furthermore, DAC does not scale well beyond small sets of users.

Role Based Access Control (RBAC) Access policy is determined by the system [5]. Where with MAC access is based on subject trust or clearance, with RBAC access is based on the role of the subject. A subject can access an object or execute a function only if their set of permissions—or role—allows it.

Mandatory Access Control (MAC) Access policy is determined by the system and is implemented by sensitivity labels, which are assigned to each subject and object [5]. A subject's label specifies its level of trust, and an object's label specifies the level of trust that is required to access it. If a subject is to gain access to an object, the subject label must dominate—be at least as high as—the object label.

Critical to implementing any of these forms of encryption is the need to manage the keys that are used to encrypt and decrypt data. In addition, identifying recovery methods for when encryption keys are lost needs to be considered. When a key is lost or not available, it is important to know what options are available to recover the data.

3.2. Security Design Patterns and Best Practices

Patterns are optimal solutions to common problems. As common problems are tossed around a community and are resolved, common solutions often spontaneously emerge [6]. Eventually, the best of these rise above the din and self-identify and become refined until they reach the status of a Design Pattern.

3.2.1. IA-07 cryptographic module authentication

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked.

3.2.2. SC-12 cryptographic key establishment & management

Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57, parts 1-3 provides detailed guidance on cryptographic key management.

3.2.3. SC-13 use of cryptography

Control: For information requiring cryptographic protection, the information system implements

cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: The applicable federal standard for employing cryptography in non-national security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management.

4. Encryption Techniques

Cryptography is a complex and secretive field. Recently, cryptography has expanded from protecting the confidentiality of private communications to including techniques for assuring content integrity, identity authentication, and digital signatures along with a range of secure computing techniques [7]. Given that range of functional utility, cryptography has been recognized as being a critical enabling technology for security in cloud computing. Focusing on data security, cryptography has great value for cloud computing. To affect cryptographic data confidentiality, plaintext is converted into ciphertext by numerous means, but the ones of practical value are all based on mathematical functions that must meet several requirements, including:

- The algorithm and implementation must be computationally efficient in converting plaintext to ciphertext, as well as in decryption.
- The algorithm must be open to broad analysis by a community of cryptographers and others.
- The resulting output must withstand the use of brute force attacks even by vast numbers of computers (such as in a computing grid or cloud).

In operation, plaintext is encrypted into ciphertext using an encryption key, and the resulting ciphertext is later decrypted using a decryption key. In Symmetric cryptography, these keys are the same. Symmetric cryptography has broad applicability, but when it is used in communication between parties, the complexity of key management can become untenable since each pair of communicators should share a unique secret key. It is also very difficult to establish a secret key between communicating parties when a secure channel does not already exist for them to securely exchange a shared secret key.

4.1. Symmetric Encryption

Symmetric Encryption protects message confidentiality by making a message unreadable to those that do not have access to the key. Symmetric encryption uses the same key for encryption and decryption [8]. By contrast, with asymmetric cryptography (also known as in public–private key cryptography), the encrypt key (public key) is different but mathematically related to the decrypt or private key.

The primary advantage of asymmetric cryptography is that only the private key must be kept secret—the public key can be published and need not be secret [3]. Although public–private key pairs are related, it is infeasible to computationally derive a private key from a public key.

4.2. Asymmetric Encryption

Asymmetric Encryption provides message confidentiality by keeping information secret in such a way that it can only be understood by intended recipients who have access to the valid key [8]. In asymmetric encryption, a public/private key pair is used for encryption and decryption respectively.

This use of public–private keys is an enabler for confidentiality in cloud computing, and not just for encryption of content [3]. A private key can be used to authenticate a user or computational component, and it can also be used to initiate the negotiation of a secure channel or connection between communicating parties.

4.3. Basic Uses of Cryptography

The four basic uses of cryptography [9] are:

- **Block ciphers:** These, take as input, a key along with a block of plaintext and output a block of ciphertext. Because messages are generally larger than a defined block, this method requires some method to associate or knit together successive ciphertext blocks.
- **Stream ciphers:** These operate against an arbitrarily long stream of input data, which is converted to an equivalent output stream of ciphertext.

- **Cryptographic hash functions:** Hash functions take an arbitrarily long input message and output a short, fixed length hash. A hash can serve various purposes, including as a digital signature or as a means to verify the integrity of the message.
- **Authentication:** Cryptography is also widely used within authentication and identity management systems.

5. Remote Data Storage Encryption

"Encryption is a key component to protect data at rest in the cloud. Employing appropriate strength encryption is important: Strong encryption is preferable when data at rest has continuing value for an extended time period [3]."
Several of the ways of encrypting data at rest are listed below.

5.1. Encryption for Data in Transit

The two goals of securing data in motion are preventing data from being tampered with (integrity) and ensuring that data remains confidential while it is in transit. Other than the sender and the receiver, no other party observing the data should be able to either make sense of the data or alter it. The most common way to protect data in motion is to utilize encryption combined with authentication to create a conduit in which to safely pass data to or from the cloud.

Encryption is used to assure that if there was a breach of communication integrity between the two parties that the data remains confidential. Authentication is used to assure that the parties communicating data are who they say they are. Common means of authentication themselves employ cryptography in various ways. Transferring data via programmatic means, via manual file transfer, or via a browser using HTTPS, TLS, or SSL are the typical security protocols used for this purpose. A PKI is used to authenticate the transaction (trusted root CAs), and encryption algorithms are used to protect the payload.

5.2. Encryption for Data at Rest

5.2.1. Full disk

Encryption of data at the disk level—the operating system, the applications in it, and the data the applications use are all encrypted simply by existing on a disk that is encrypted. This is a brute-force approach to encrypt data since everything is encrypted, but this also entails performance and reliability concerns. If encryption is not done at the drive hardware level, then it can be very taxing on a system in terms of performance. Another consideration is that even minor disk corruption can be fatal as the OS, applications, and data.

5.2.2. File system

In this use of encryption, entire data directories are encrypted or decrypted as a container. Access to files requires use of encryption keys. This approach can also be used to segregate data of identical sensitivity or categorization into directories that are individually encrypted with different keys.

5.2.3. File level

Rather than encrypting an entire hard drive or even a directory, it can be more efficient to encrypt individual files.

5.2.4. Application level

The application manages encryption and decryption of application-managed data.

5.3. Deletion of Data

When removing data from a cloud provider it is important to understand how that data is deleted [10].

5.3.1. Clearing

Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored

information.

5.3.2. Sanitization

Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.

5.4. Data Masking

Data masking is a technique that is intended to remove all identifiable and distinguishing characteristics from data in order to render it anonymous and yet still be operable [3]. This technique is aimed at reducing the risk of exposing sensitive information. Data masking has also been known by such names as data obfuscation, de-identification, or depersonalization. These techniques are intended to preserve the privacy of records by changing the data so that actual values cannot be determined or re-engineered. A common data masking technique involves substitution of actual data values with keys to an external lookup table that holds the actual data values. In operation, such resulting masked data values can be processed with lesser controls than if the original data was still unmasked.

6. Standardization

Cloud services are relatively new in the world of technology. Because of the lack of standards it can impede the adoption of cloud services. There aren't really any official standards with respect to who controls all cloud services and/or the way that they're managed. There are some emerging standards. So with respect to some of the background and/or the current status of cloud services, there is no single authoritative cloud standards body.

There are many proprietary application programming interfaces (APIs) that have been adopted as de facto standards, but without any kind of official general industry agreement. Amazon Web Services, one of the standard providers, have been widely adopted as a *de facto standard*. Among the people who are developing within cloud services AWS has become something that's fairly common, but it is still yet to achieve any kind of official standardization. The field is large and the below standards bodies each have contributed with their own interpretations.

6.1. Cloud Security Alliance (CSA)

The Cloud Security Alliance provides a security guidance document, which is founded on continuous observation of applicable standards in all of the 14 identified domains of consideration. They publish the security guidance for critical areas of focus in cloud computing and a cloud control matrix.

http://www.cloudsecurityalliance.org/

https://cloudsecurityalliance.org/research/cloud-controls-matrix/

The CSA also maintains the security, trust, and assurance registry; a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of providers and consumers and is used by customers, providers, industries, and governments.

6.2. OMG Standards Development Organization

The Object Management Group® (OMG®) is another organization that publishes a number of guidance papers to develop awareness, adoption, and standardization of cloud services [11]. The OMG® is an umbrella organization promoting and supporting cloud standards and cloud direction.

It is an ***end user advocacy group*** dedicated to accelerating the cloud's successful adoption, and drilling down into the standards, security, interoperability, and various other issues that are surrounding any kind of transition to the cloud.

https://www.omg.org/about/omg-standards-introduction.htm

6.3. International Standards Organization (ISO)

The International Standards Organization 27XXX is an application of ISO and IEC in the cloud environment. It deals with Information Technology Systems Management. The Working title, Service Management Part 7, is guidance on the application of ISO/IEC to the cloud. It is hoped that this will become

an international standard that will give guidance on the application as it applies to cloud computing.

6.4. National Institute of Standards and Technology (NIST)

U.S. based cloud computing program designed to provide leadership and guidance around cloud computing and promote adoption within the industry and government to encourage the adoption of cloud computing [12]. Nothing has been officially adopted, but several U.S. governmental agencies have adopted it. There is still no governing body, but at least we're seeing organizations that are interested in promoting this type of technology and education. Like many things, it does require research particularly if the organization requires a lot of regulatory compliance.

6.5. Institute of Electrical and Electronics Engineers (IEEE)

The IEEE has a number of standards that exist in the IT world. P2301, Cloud Profiles, provides information for different cloud participants, such as the cloud vendors, service providers, and users. P2302, Intercloud, defines topology, functions, and governance for cloud-to-cloud interoperability and federation [13].

7. Conclusions and Recommendations

There have been many advances in the cloud security world, but still there are no straightforward approaches for cryptographic implementation. Shared ownership of cloud assets and stored data has made it increasingly difficult to draw the lines of demarcation between provider and consumer. The symbiotic relationship between provider and consumer continues to be a point of contention for public cloud adoption.

If information in the cloud is to be confidential, then encryption can certainly handle that. If the need is to ensure that the data is intact, not been tampered with, then something like a digital signature or a hashing algorithm can ensure that integrity. Cryptography also provides authentication, validating which entity you might be dealing with, non-repudiation, which insures that a person cannot refute themselves from this specific type of action. It can also provide access control ensuring that only the appropriate entities are able to gain access to this information.

Adopters of public cloud computing environments must have a strategy to provide confidentiality and integrity of the data that resides outside of the confines of their own datacenters. Correctly implementing cryptography is the means for them to accomplish that task.

Conflict of Interest

The author declares that they have no conflict of interest.

References

[1] N. Lord. (2018). *DigitalGuardian DataInsider-Cryptography in the Cloud: Securing Cloud Data with Encryption.* [Online]. Available: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption

[2] NIST Special Publication 800-146-Cloud Computing Synopsis and Recommendations. (2012). [Online]. Available: Retrieved from https://csrc.nist.gov/publications/detail/sp/800-146/final

[3] J. Winkler, *Securing the Cloud: Cloud Computer Security Techniques and Tactics*, Syngress Publishing, pp. 136–145, 2011,

[4] NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing. (2011). [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-144/final

[5] S. Harris and F. Maymi, *CISSP® All-in-One Exam Guide,* Seventh Edition, The McGraw-Hill Companies, 2016.

[6] E. Fernandez-Buglioni, *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*, John Wiley & Sons, 2013.

[7] OSA Security Patterns Control Catalog. (2018). [Online]. Available: http://www.opensecurityarchitecture.org/cms/library/0802control-catalogue/186-08-02-ia-07

[8] Microsoft Learn- Encrypting Data. (2022). [Online]. Available: https://learn.microsoft.com/en-us/dotnet/standard/security/encrypting-data

[9] H. Murti, E. Lestariningsih, R. Redjeki, and E. Ardhianto, "Systematic literature review of the role of fuzzy logic in the development of cryptographic and steganographic techniques," *Asian Journal of Research in Computer Science*, 2021.
[10] T. Maher, S. Kumaraswamy, and S. Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Rielly Media, Inc., pp. 64–66, 2009,
[11] OMG Standards Development Organization- Security for Cloud Computing Ten Steps to Ensure Success Version 3.0. [Online]. Available: https://www.omg.org/cloud/deliverables/security-for-cloud-computing-10-steps-to-ensure-success.htm
[12] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations. (2020). [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[13] IEEE Standard 2302-2021- IEEE Standard for Intercloud Interoperability and Federation (SIIF). (2022). [Online]. Available: https://standards.ieee.org/ieee/2302/7056/