International Journal of
Science and Engineering Investigations vol. 8, issue 85, February 2019
Received on February 18, 2019 ISSN: 2251-8843

Applying Cryptography to Ensure Cloud Computing Security

Pee Vululleh
Ph.D., Faculty, Regent University
(nohson16@yahoo.com)

Abstract-Described in basic terms, cloud computing is the delivery of computer services-storage, applications, and processing power-through cloud service providers typically via the cloud (the Internet) on a pay as you go basis. As cloud computing has evolved, it has develop in the form of three computing models: cloud applications or software as a service (SaaS), Cloud platform services or Platform as a service (PaaS), and cloud infrastructure services or infrastructure as a service (IaaS). The delivery of services (i.e., storage and applications) as services and not as products, offers cost efficient and faster innovation. The versatility that cloud computing technology provides is one of its biggest benefits. Organizations benefit from a great deal of flexibility, as Internet-based delivery makes it possible to access data from virtually anywhere and from any network-attached computer or devices. The paper explains that basis of cryptography security by exhibiting some security issues of cloud computing in today's environment. This also paper focuses on understanding by proposing effective measures and crypto algorithms to ensure the security of cloud data.

Keywords- *Cryptography, Security, Cloud Computing*

I. INTRODUCTION

Due to the necessity for organizations computing on-the-go, cloud computing represents the next-generation paradigm in computation. In the cloud computing environment, computer services-applications, storage, and processing power are delivered through cloud service providers on a pay-as-you-go basis over the Internet [8]. In simplest terms, cloud computing is similar to an electrical power grid delivery system. To an average computer user, cloud computing offers the advantage of delivering technology's services without requiring the user to have an in-depth knowledge of the technology itself, which is similar to the way a customer can access electricity without knowledge of polarity and grids.

Despite the many advantages of the cloud computing environment, there are many security issues to resolve. For example, unauthorized third party access to an organization's data is a major issue in cloud computing [11]. Proper encryption of data using crypto-algorithms such as Rivet-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish can help to make it harder for unauthorized third parties to decrypt, access, and steal data [9]. Encryption algorithms perform processes that transform message into ciphertext. Encryption techniques are classified into two groups, namely, Symmetrickey, executed using algorithms such as AES, DES, 3DES and Bluefish, on the one hand, and Asymmetric key is executed using algorithms such as RSA and Diffie-Hellman, on the other [3] [12]. The use of algorithms places data into meaningless cipher-text and requires the use of a key to transform the data back to its original state. This paper focuses on understanding the issues surrounding cloud security by proposing effective measures and crypto algorithms to ensure the security of data in a cloud computing environment.

II. RELATED WORKS

[4] Proposed a mathematical model of the user's trust using RSA and AES. [5] Presented an approach to modeling security requirements for cloud-stored data in the least amount of time and cost efficient encryption and decryption processes. [10] Employed RSA and AES to introduce a backbone structure for cloud storage.

III. CRYPTOGRAPHY

For organizations that are reluctant to use cloud computing due to security concerns, cryptography can help eliminate some of those concerns. Cryptography in cloud computing employs encryption mechanisms to safeguard data that is in use or stored in the cloud and, as encryption protects any data that is hosted by cloud service providers, allows organizations to access shared cloud services securely and conveniently. Cryptography in the cloud secures critical data beyond the corporate IT setting, where that data is no longer under corporate IT control. Cryptography considers three algorithms, namely, symmetric key algorithms, asymmetric key algorithms, and hashing [6]. Problems in data security, network traffic, backup data, and file storage system are major concerns in cloud computing, concerns that cryptography alone can solve to some extent [1]. For example, encryption can help to protect consumer confidential data stored in the cloud. [15] [7]. Recommended not to save an encrypted key on the same server as data is stored in order to reduce the vulnerability of virtualization. Some organizations choose to encrypt data before uploading it to the cloud altogether. This method is beneficial, because encryption takes place before data leaves the organization's environment, and thereafter only authorized parties have access to the appropriate decryption keys. Other

services perform encryption of data upon receipt, certifying that any transmitted or stored data is protected by encryption by default. Cloud services that do not offer encryption capabilities should, at the very least, use encryption technologies such as virtual private networks (VPNs), HTTPS, and secure shell (SSH) to ensure that data is secured in transit [2].

Cloud computing offers users a virtual computing infrastructure within which they are able to store data and run applications. However, cloud computing comes with security challenges, because cloud service providers handle and store clients' data beyond the reach of their existing security measures. A cryptographic approach has been widely used to overcome these challenges by ensuring data security and trust in cloud computing.

A. Symmetric Encryption

Symmetric encryption (Secret key) uses single key and is considered to be one of the simplest and fastest encryption techniques [13]. The single key is used to both encrypt and decrypt the data [16]. Sharing the sky is the biggest drawback with symmetric key encryption. However, symmetric encryption is particularly useful when encrypting an organization's own cloud data as opposed to sharing encrypted data with a third party. Common symmetric encryption algorithms include AES, DES, 3DES, and Blowfish

B. Advanced Encryption Standard

Advanced Encryption Standard (AES) is the most widely used algorithm in symmetric key cryptography. It comprises three block ciphers, AES 128, 192, and 256, each of which is considered sufficient to protect data ranging from classified to top secret security levels [3] [14]. If integrity and confidentiality are major concerns, the AES algorithm can be used. To date, practical cryptanalytic attacks against AES have been nonexistent. Additionally, AES's key length built-in flexibility allows for a degree of future proofing against progress in the capacity to perform full-scale key searches. However, the security of AES is guaranteed only if it is properly applied and good key management is utilized.

C. Data Encryption Standard (DES)

DES is a symmetric encryption-key block cipher published by the National Institute of Standards and Technology in 1977. The technology is an implementation of the Feistel Cipher, which uses a 16 round Feistel structure with a block size of 64 bits [13] [14]. Eight of the 64 bits of key function are check bits, making DES effective with a key length of 56 bits. DES satisfies both the desired properties of a block cipher. DES is the best option if the application demands significant network bandwidth. Avalanche effect and completeness make the cipher extremely strong. With the Avalanche effect, $_{a}$ minor change in plaintext results in a significant change in the ciphertext and with completeness, each bit of ciphertext depends on many bits of plaintext. During the last few years, cryptanalysts have observed some weaknesses in DES, especially when the key selected is a weak key [6]. In order for DES to be effective, weak keys should be avoided. DES has seen no significant cryptanalytic attacks other than full-scale key search.

D. Blowfish

Blowfish uses block cipher with 64 bits and 32 bits to 448 bits of variable key length and is much faster than DES [12]. The Blowfish algorithm standard is best in case of memory and time. Both blowfish and AES encryption standards are used to prevent guessing attacks and can be applied to IPv4 IPv6-based Internet protocols.

E. Asymmetric Encryption

Asymmetric encryption (public key encryption) uses two interdependent keys, one for encryption purposes and the other for decryption purposes. The keys' interdependency provides a number of unique features, including digital signatures, which are used amongst other things to guarantee that a message originated from a particular entity or users to authenticate remote.

F. Diffie-Hellman Key Exchange

The Diffie-Hellman key exchange (DHKE) is one the most commonly used asymmetric encryption algorithms. DHKE allows for the exchange of cryptographic keys in a secure manner regardless of whether communication channels are private or public.

G. Rivest-Shamir-Adleman

Rivest-Shamir-Adleman (RSA) is another widely used asymmetric algorithm encryption technique for use with electronic commerce protocols such as SSL. It is considered to be secure because of its use of up-to-date implementations and sufficiently long keys [12] [14].

H. Hashing Function

Cryptographic hash functions compare differently to other cryptographic algorithms. Hash functions are used to return a value based on a file, message, or piece of data. Any intentional or accidental change in the data causes a change in hash value (message digest). Good hash algorithms should make possible the creation of an initial input that produces a fixed message digest or allows the message digest to calculate the original input.

IV. CLOUD COMPUTING SECURITY ISSUES

Efficient, scalable, and affordable cloud computing is still the best solution for most organizations, but its use can still leave them vulnerable if the proper precautions are not applied. There is several cloud computing security risks, but the most common are:

1. **Distributed Denial-of-Service Attacks:** Initiation of enough traffic to a cloud computing system can result in either temporary or indefinite disruption of services.
2. **Shared Cloud Computing Services:** Many cloud solutions do not provide the required security between clients, which can lead to shared systems, resources, and applications. In this scenario, threats can emerge from other clients of a cloud computing service and could as well affect other clients.

3. **Employee Negligence:** Employee mistakes and negligence remain one the biggest security issues for all systems, including cloud computing solutions. Today, employees are able to log into cloud systems using their home tablets, home PCs, and mobile phones, potentially introducing external vulnerabilities into the system.
4. **Inadequate Data Backups and Data Loss:** Improper data syncing and inadequate data backups have made several organizations vulnerable to ransomware, which is a specific type of cloud computing security threat. The threat (ransomware) encrypts an organization's data file and only allows access to it after the owner pays ransom. With proper data backup solutions, organizations should be able to avoid being placed in a ransomware situation.
5. **Social Engineering and Phishing Attacks**: Once confidential or login information is acquired, a hostile user can easily access a system. Employees must receive adequate awareness training about social engineering and phishing so that they can fend off such attacks.
6. **System Vulnerabilities**: Cloud computing systems can be vulnerable, especially in networks that have multiple third-party platforms and complex infrastructures. Once vulnerability becomes known with a popular third-party system, it can easily be used to attack an organization's assets. Proper update protocols, network monitoring solutions, and patching are critical to fighting the threats.

Cloud security issues are not too great to be overcome. Organizations can protect themselves from several of the previously mentioned risks through the utilization of a data protection services. Cloud computing data protection solutions can both protect data against cyber security threats and loss, allowing organizations to enjoy the benefits of cloud services with a minimum of risk.

V. CONCLUSION

Cloud computing is a growing next-generation paradigm in computation. In the cloud computing environment, computer services such as applications, storage, and processing power are delivered through cloud service providers on a pay-as-you-go basis over the Internet. Despite the many advantages of cloud computing, there are many security issues in the cloud computing environment. Proper encryption of data using crypto algorithms such as Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish can help to protect against the security threats that have emerged in connection with the technology.

REFERENCES

[1] AbdElnapi, N., Omara, F., & Omran, N. (2016). A hybrid hashing security algorithm for data storage on cloud computing. International Journal of Computer Science and Information Security, 14(4), 175. doi:10.5815/ijcnis.2017.06.06

[2] Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4), 485-498. doi: 10.14569/IJACSA.2016.070464

[3] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[4] Bokefode Jayant, D., Ubale Swapnaja, A., Pingale, S., Pingale Subhash, V., Karande Kailash, J., & Apate , S. (2015). Developing secure cloud storage system by applying AES and RSA cryptography algorithms with role based access control model. International Journal of Computer Applications, (0975–8887) Volume. doi:10.5120/20801-3484

[5] Chandar, R., Kavitha, M., & Seenivasan, K. (2014). A PROFICIENT MODEL FOR HIGH END SECURITY IN CLOUD COMPUTING. 4(2). Retrieved from https://core.ac.uk/download/pdf/25558249.pdf

[6] Hossain, M., Hossain, M., Uddin, M., & Imtiaz, S. (2016). Performance Analysis of Different Cryptography Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3). Retrieved from https://pdfs.semanticscholar.org/a88e/e53f725bf25537dd7c272fb032fb5d638fa7.pdf

[7] Hur, J., Koo, D., Shin, Y., & Kang, K. (2016). Secure data deduplication with dynamic ownership management in cloud storage. IEEE Transactions on knowledge and data engineering, 28(11), 3113-3125. doi:http://doi.ieeecomputersociety.org/10.1109/TKDE.2016.2580139

[8] Jouini, M., & Rabai, L. (2016). A security framework for secure cloud computing environments. International Journal of Cloud Applications and Computing (IJCAC), 6(3), 32-44. doi: 10.4018/IJCAC.2016070103

[9] Khan, S., & Tuteja, R. (2015). Security in cloud computing using cryptographic algorithms. International Journal of Innovative Research in Computer and Communication Engineering, 3(1), 148. Retrieved from http://www.ijircce.com/upload/2015/january/23E_Security.pdf

[10] Pitchay, S., Alhiagem, W., Ridzuan, F., & Saudi, M. (2015). A proposed system concept on enhancing the encryption and decryption method for cloud computing. In Modelling and Simulation (UKSim), 2015 17th UKSim-AMSS International Conference on, (pp. 201-205). IEEE.

[11] Samarati, P., di Vimercati, S., & Murugesan, S. (2016). Cloud security: Issues and concerns. Encyclopedia on cloud computing, 207-219. doi: https://doi.org/10.1002/9781118821930.ch17

[12] Shi, W., & Dustdar, S. (2016). The promise of edge computing. Computer, 49(5), 78-81. doi:10.1109/MC.2016.145

[13] Stergiou, C., Psannis, K., Kim, B., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future Generation Computer Systems, 78, 964-975. doi:http://dx.doi.org/10.1016/j.future.2016.11.031

[14] Wahid, M., Ali, A., Esparham, B., & Marwan, M. (2018). A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technology, 2(3), 1-7. doi:DOI: 10.15226/2474-9257/3/2/00132

[15] Yan, Z., Ding, W., Yu, X., Zhu, H., & Deng, R. (2016). Deduplication on encrypted big data in cloud. IEEE transactions on big data, 2(2), 138-150. doi:10.1109/TBDATA.2016.2587659

[16] Yan, Z., Li, X., Wang, M., & Vasilakos, V. (2017). Flexible data access control based on trust and reputation in cloud computing. IEEE Transactions on Cloud Computing, 5(3), 485-498. doi:http://doi.ieeecomputersociety.org/10.1109/TCC.2015.2469662

How to Cite this Article:

Vululleh, P. (2019). Applying Cryptography to Ensure Cloud Computing Security. International Journal of Science and Engineering Investigations (IJSEI), 8(85), 74-76. http://www.ijsei.com/papers/ijsei-88519-12.pdf