©2022 Published in 10th International Symposium on Innovative Technologies in Engineering and Science 21-23 October 2022 (ISITES2022 Bursa - Turkey)
https://doi.org/10.33793/acperpro.05.03.4891

Implementation of Shamir's Secret Sharing Scheme in Cloud Computing

*[1]Betul Karaoglan and [1]Muhammet Tahir Guneser
*[1]Faculty of Engineering, Department of Electrical and Electronics Engineering Karabuk University, Turkey

Abstract

With the increase in the use of cloud systems, security on cloud systems has become one of the most important items that underlined. Due to the nature of the cloud systems, it is difficult to manage multi-user systems and access control devices, resulting in some security vulnerabilities. In this paper we studied on Cloud Computing with Shamir's Secret Sharing Scheme with Advanced Encryption Standard (AES) algorithm for encryption and decryption process. For encryption and decryption process AES in Cryptool 1.4.41 has been used. For implementing Shamir Secret Sharing Scheme, Python language has been chosen and Spyder 3.8 has been chosen for environment. As a result, we successfully demonstrate the Shamir's Scheme implementation with file operations.

Key words: Cloud computing, data security, secret sharing, Shamir's Scheme

1. Introduction

In today's technology, users want to store more and more data every day. With the limitations of current devices, usage of clouds is increasing day after day. Thanks to cloud computing, it is possible to access the requested information from anywhere and using any kind of information communication device (PC, Mac, iPhone, Android, etc.). The lack of hardware-related problems, the ability to offer high availability through the virtual computer running faster than physical servers, the use of flexible structure that does not require memory and disc change, and the nature-friendly (electricity and space saving) are the first and foremost advantages of cloud computing [1]. Considering all these advantageous aspects; it is not seen as a rational solution to stay away from cloud computing which is the reflection of the development in information communication technologies or to insist on alternative methods. But the risks associated with cloud computing cannot be ignore [2]. Compared to other schemes Shamir's Secret Sharing Scheme provides more security because, cannot rebuilt the original data with less than the needed shares [3]. Previous works demonstrate that, cloud-based imaging with Shamir's Scheme provide data confidentiality, availability, and integrity [4]. We implemented Shamir's Scheme for file storage in multiple clouds.

In this study we implemented system that first create encrypted hex file with CrypTool, then python program takes that hex file as input and creates n shares. With k shares reconstructed hex file then this output file tested with CrpTool. CrpTool used for testing AES encryption and decryption processes. With this approach, system provides data confidentiality, data availability and data integrity.

*Corresponding author: Address: Faculty of Engineering, Department of Electrical and Electronics Engineering Karabuk University, 78000, Karabuk TURKEY. E-mail address: betulkaraogran@karabuk.edu.tr, Phone: +903704187213

In the following sections of this study, firstly brief information about cloud computing and security problems will be given. Then, Shamir's Secret Sharing Scheme and its usability of cloud security will be discussed.

2. Cloud Computing

Cloud computing, which has emerged as a solution to the growing need for data storage, now serves many users today. Cloud technology established and shared by large organizations. Using this technology, reduces the accountability on personal computers. Also, number of applications are provided by the cloud server. All the applications, programs and data we host on the internet store in the cloud. Any device connected to internet can easily access this information [1].

The clouds have different architecture based on the services they provide. The data stored on the data centres and it can be processing anywhere on servers. So, users must trust the service provider for availability and security of data. The Service Level Agreement (SLA) is the only legal agreement between provider and users [5]. SLA describes the service; document Service Targets and defines the responsibilities of the provider and user. With this agreement, user takes the all the responsibility for data loss or corruption [6].

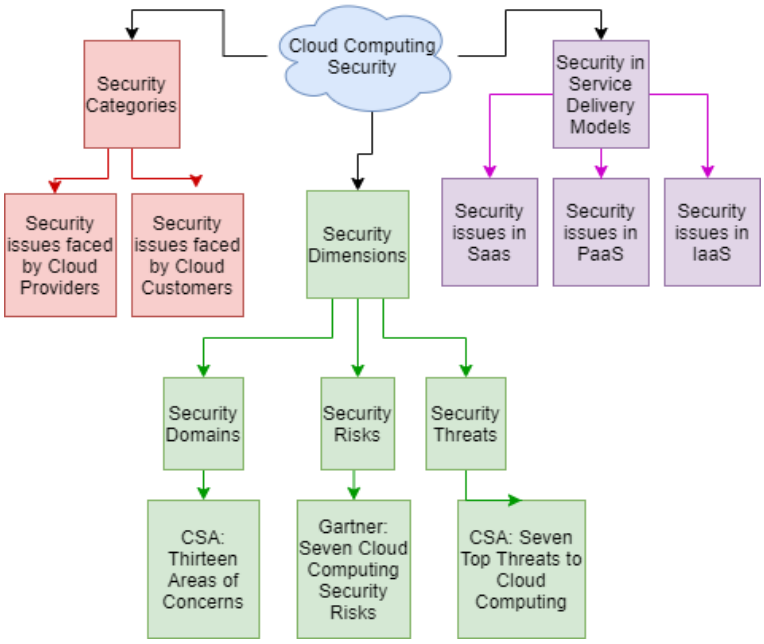

Figure 1. Cloud computing security [10]

2.1. Cloud Service Models

Cloud technology offers flexible and diverse service services that can be used in accordance with the wishes and needs of the user, rather than a strict and standardized structure [7]. These cloud services, which are within the scope of cloud technology, consist of three structures in general: Infrastructure as a Service, Platform as Service and Software as Service.

2.1.1. Infrastructure as a Service (IaaS):

In the cloud technology infrastructure, it is used to refer to the services in the lowest layer [8] [9]. In the infrastructure service model, organizations provide their needs such as the storage device, computer network and server they need for the enterprise from the companies that provide cloud services as a service, in other words, virtual hardware is provided to the user.

2.1.2. Platform as a Service (PaaS):

The service provider provides the user with an environment in which he can develop and operate his own application, as well as a platform that includes complementary services and the necessary technological infrastructure [8] [9]. Apart from the application established by the user himself, there is no control and management possibility on the components of the platform infrastructure. This service can be considered as renting hardware, operating system, storage unit and network capacity over the Internet.

2.1.3. Software as a Service (SaaS):

In this service model, users can work by accessing applications on the cloud from any location to connected to the internet without any installation to their systems. The service provider's software runs on the cloud infrastructure [8] [9]. Applications can be accessed from various user devices (desktop, laptop, tablet, mobile phone, etc.) without any time and location restrictions through interfaces such as web browsers thanks to the internet connection. Users do not manage or control components such as network, server, operating system, and storage devices in the infrastructure [9]. Only user-specific application settings can be made.

2.2. Cloud Security

While cloud computing has many advantages, there are some potential problems encountered in services [10] [11] [12]. Majority of these problems can be considered as compliance with local or regional regulations, the need to obtain approval in areas that are not authorized to access, some additional complexities in terms of supervision, the need to repair according to the nature of the cloud, and the lack of trust that can be detected in cloud services.

Cloud computing security is related to the security of the data and applications of cloud users and service servers, methods, rules and technologies used to secure the infrastructure used for cloud computing. Requirements for ensuring cloud security are provided by default system security mechanisms defined by the cloud infrastructure, data access control mechanisms agreed upon by users and service providers, service level access agreements, and additional security functions provided by the service used [10]. The most important of the cloud security requirements are data privacy, data integrity, authentication, and identity management, physical and personal security, accessibility, security of application service, privacy, and compliance with the law [11]. Cloud security can be threatened by insecure applications, malicious insiders, untrusted 3rd parties [12]. Shamir' Secret Sharing Scheme with AES can be used for overcome these problems.

3. Shamir's Secret Sharing

As a result of digitalization, the biggest difficulty that we face is the problem of safe transmission of data. Secret Sharing Scheme is one of the most known techniques that interested of secure data transmission. Which focus on key distribution and management [14].

(k, n) Threshold scheme was first proposed by Shamir and Blakley in 1979. Methods share confidential data between n participants [14]. Confidential data can be obtained by gathering any one or more of the participants. There is no possibility to obtain information about confidential data by using fewer than keen shares. Shamir's scheme is based on polynomial interpolation while Blakley's method uses plane geometry [15]. Basic explanation of Shamir's Secret Shamir Scheme shown in Fig. 2.

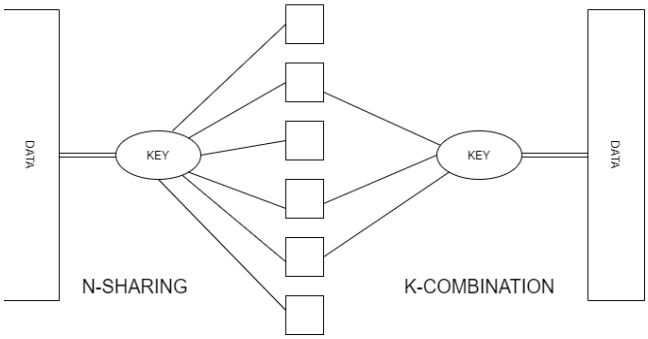

Figure 2. Basic explanation of Shamir's Secret Sharing Scheme

4. Proposed Approach

To prevent data loss in cloud we should encrypt data. But only encryption is not completely providing security. If data in the cloud, loss or corrupted; users cannot access data correctly. According to SLA, provider does not take any responsibility [5]. This causes a lack of trust for cloud computing. To solve this problem, we suggest a new approach to store data. Firstly, data encrypted with AES(CBC) then encrypted data separate with n shares. K combination of n shares reconstructs the original data [15]. AES (CBC) working principle is shown in Fig.3. and Fig.4. Fig.3. is encryption process and Fig.4. is decryption process. In Fig.5. tested system is shown. Data file encrypted with CrypTool AES(CBC). Encrypted file has been processed with our Shamir Secret Sharing algorithm. In the algorithm we read the data file and calculate the n points for sharing. After calculating the shares, k combination of shares are combined and original data is being reconstructed. Then, reconstructed data decrypted with AES(CBC).

We assume that our data is equal to 4311 (S=4311) and we have 6 different cloud to store this data (n=6). To implement of Shamir's Secret Sharing Scheme to shown in Fig.6., we determine the combination number to 3 (k=3). We need k-1 numbers which are 418 and 40 for construction of equation. When we constructed this values in (1), our polynomial equation equal to (2).
To strengthen to security, we calculate polynomial points as (3) instead of (4) [14]. Where p is prime number and p is greater and s and n. In this case our p value is equal to 16111.

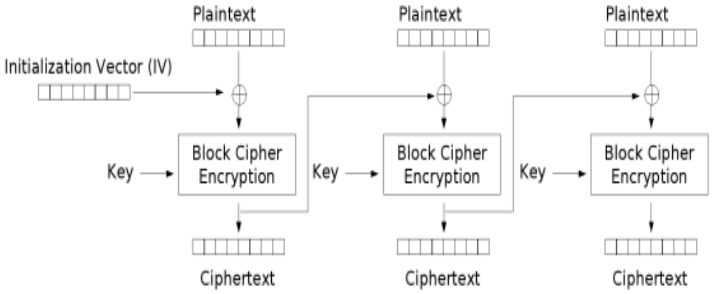

Figure 3. AES (CBC) Encryption

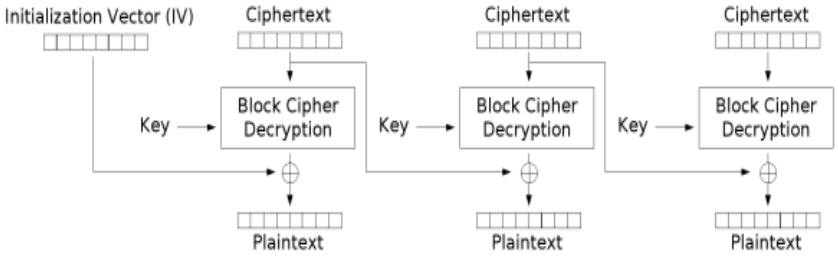

Figure 4. AES (CBC) Decryption

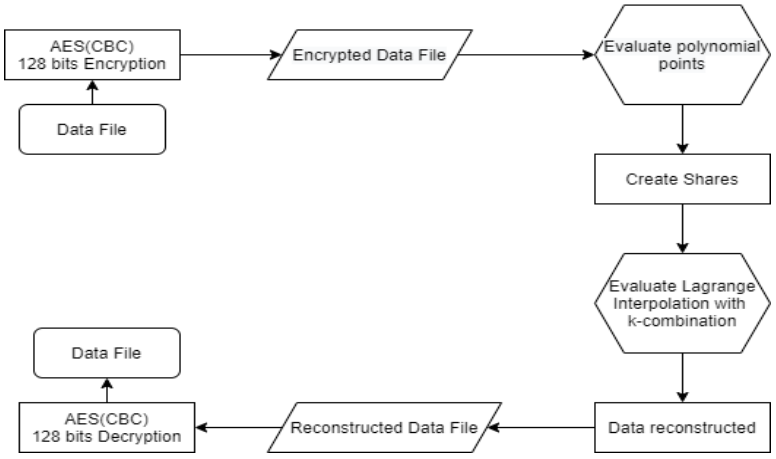

Figure 5. Tested system flowchart

Therefore, we get (5). We divide 6 points in (5) as (6), (7), (8), (9), (10), (11). So, we divide our data 6 pieces and store them different clouds. To reconstruct original data, we need at least 3 points. These 3 points can be chosen randomly. We choose (7), (9) and (10). After choosing 3 points, we use Lagrange basis polynomials and obtain (15), (16), (17). Therefore, applying (18) with (15), (16) and (17) we got (19). As a result of (19), we successfully reconstruct original data (secret) 4311 with Shamir' Secret Scheme shown in (20). Use finite field arithmetic with Shamir's Secret Scheme, provides perfect security [14] [17]. However, previous works shows that this system still need to be tested in real cloud environment with different file size, types and threshold values [18].

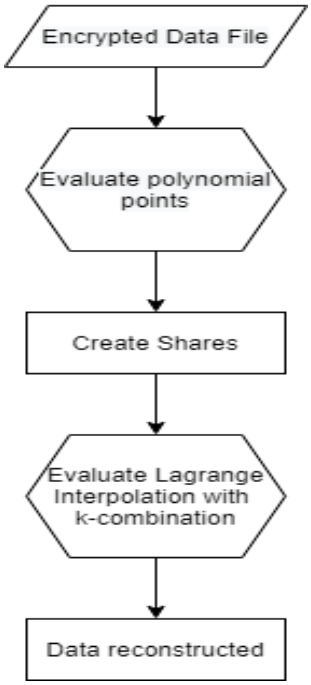

Figure 6. Shamir's Secret Sharing algorithm processes

$$f(x) = a_0 + a_1 x + a_2 x^2 \quad (1)$$

$$f(x) = 4311 + 418x + 40x^2 \quad (2)$$

$$D_x = (x, F(x) mod p) \quad (3)$$

$$D_x = (x, F(x)) \quad (4)$$

$$D_x = (x, F(x) 16111) \quad (5)$$

$$D_1 = (1,4769) \quad (6)$$

$$D_2 = (2,5307) \quad (7)$$

$$D_3 = (3,5925) \quad (8)$$

$$D_4 = (4,6623) \quad (9)$$

$$D_5 = (5,7401) \quad (10)$$

$$D_6 = (6,8259) \quad (11)$$

$$(x_0, y_0) = (2,5307) \quad (12)$$

$$(x_1, y_1) = (4,6623) \quad (13)$$

$$(x_2, y_2) = (5,7401) \quad (14)$$

$$l_0 = \frac{x-x_1}{x_0-x_1} \cdot \frac{x-x_2}{x_0-x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{x^2-9x+20}{6} \quad (15)$$

$$l_1 = \frac{x-x_0}{x_1-x_0} \cdot \frac{x-x_2}{x_1-x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = \frac{-x^2+7x-10}{2} \quad (16)$$

$$l_2 = \frac{x-x_0}{x_2-x_0} \cdot \frac{x-x_1}{x_2-x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{x^2-6x+8}{3} \quad (17)$$

$$f(x) = \sum_{j=0}^{2} y_j \cdot l_j(x) = y_0 \cdot l_0 + y_1 \cdot l_1 + y_2 \cdot l_2 (18)$$

$$5307 \cdot \left(\frac{x^2-9x+20}{6}\right) + 6623 \cdot \left(\frac{-x^2+7x-10}{2}\right) + 7401 \cdot \left(\frac{x^2-6x+8}{3}\right) \quad (19)$$

$$4311 + 418x^2 + 40x^2 \quad (20)$$

Conclusion

The purpose of this study examines cloud computing and to achieve strong security for cloud computing with using secret sharing. Studies shows that, using Shamir's Secret Sharing for cloud storage provides more security and integrity in theory and practice. This project implemented in Spider 3.8 Python. First, Cryptool 1.4.41 used to obtain encrypted data file. 128-bit AES encryption is used. Then encrypted data used for evaluating 6 polynomial points. 3 points used for reconstruction. Reconstructed data file decrypted with CrypTool and original data obtain successfully. For future works, implementing system with real cloud systems can be done.

Acknowledgements

In this study digital library facilities of University of Karabuk are used.

References

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[2] Hourani, H., & Abdallah, M. (2018, July). Cloud computing: legal and security issues. In: 8th International Conference on Computer Science and Information Technology (CSIT) (pp. 13-16). IEEE.

[3] Pundkar, S. N., & Shekokar, N. (2016, March). Cloud computing security in multi-clouds using Shamir's secret sharing scheme. In: International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 392-395). IEEE.

[4] Mohanty, M. (2013). Secret sharing approach for securing cloud-based image processing.

[5] Kandukuri, B. R., & Rakshit, A. (2009, September). Cloud security issues. In: IEEE International Conference on Services Computing (pp. 517-520). IEEE.

[6] Morin, J. H., Aubert, J., & Gateau, B. (2012, January). Towards cloud computing SLA risk management: issues and challenges. In: 45th Hawaii International Conference on System Sciences (pp. 5509-5514). IEEE.

[7] Shirvani, M. H. (2018, July). Web Service Composition in multi-cloud environment: A bi-objective genetic optimization algorithm. In: Innovations in Intelligent Systems and Applications (INISTA) (pp. 1-6). IEEE.

[8] Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In The 33rd international convention mipro (pp. 344-349). IEEE.

[9] Aksakallı, İ. K. (2019). Bulut Bilişimde Güvenlik Zafiyetleri, Tehditleri ve Bu Tehditlere Yönelik Güvenlik Önerileri. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 5(1), 8-34.

[10] Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135.

[11] Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6), 833-851.

[12] Kaul, A., Tuli, S., & Jain, R. (2014, March). Combining encryption and stego-Object processing: A new direction in cloud security. In: Conference on IT in Business, Industry and Government (CSIBIG) (pp. 1-4). IEEE.

[13] Arda, D. (2011). Kodlama teorisinin kriptografik açıdan incelenmesi, PhD Thesis.

[14] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

[15] Alam, M. K. (2013). An approach secret sharing algorithm in cloud computing security over single to multi clouds.

[16] Tompa, M., & Woll, H. (1989). How to share a secret with cheaters. journal of Cryptology, 1(3), 133-138.

[17] Pilaram, H., Eghlidos, T., & Toluee, R. (2021). An efficient lattice-based threshold signature scheme using multi-stage secret sharing. IET Information Security, 15(1), 98-106.

[18] Alsolami, F., & Boult, T. E. (2014). CloudStash: using secret-sharing scheme to secure data, not keys, in multi-clouds. In: 11th International Conference on Information Technology: New Generations (pp. 315-320). IEEE.