J. Sustain. Wireless Syst., vol. 02, no. 3, pp. 118-122
https://doi.org/10.36548/jsws.2020.3.002

A Novel Encryption and Decryption of Data using Mobile Cloud Computing Platform

Dr. Jennifer S. Raj,
Department of ECE,
Gnanamani College of Technology,
Namakkal, India.
Email: jennifer.raj@gmail.com.

Abstract- As the need for super-fast mobile devices incorporating cloud computing technology continues to be the need of the hour, Mobile Cloud Computing (MCC) serves as the platform for mobile users to share data with others, store information on the cloud and also compute using the data. Over the years, the most widely preferred encryption that has proven to be reliable is Attribute Based Encryption (ABE). However, this encryption methodology requires expensive pairing operation which makes it unsuitable for MCC. As a result of this, MCC remains slow in reaching the crowd due to the challenge of resource-constrained mobile devices. To tackle this resource-constraint we propose a novel method of outsourcing operations to resource-rich cloud servers so that the constraint on resources does not hinder proper functioning of the mobile device. There are a number of advantages when data sharing is incorporated with lightweight fine-grain data sharing methodology. This method has a number of advantages such as CCA security level, resisting decryption key exposure and supporting verifiable outsourced decryption. Simulation results indicate that the performance analysis and concrete security proof is apt for MCC environment.

Keywords: CCA secure; outsourced decryption; mobile cloud computing; attribute-based encryption; decryption.

1. Introduction

Cloud computing has gained great popularity in the recent years, in a number of fields like entertainment, education, medical treatment, economic finance and scientific research. As the need for data storage becomes a hassle, consumers are slowing migrating to the use of cloud computing which helps organizations and individuals to share, manipulate, maintain and store information. As the use of mobile devices has seen a surplus increase in usage and necessity during the past two decades, there is also much progress in the wireless communication technology and electronic technique that is used. This has led to the use of mobile phones in various applications such as mobile health monitoring, mobile learning, mobile commerce, mobile banking etc. Though the mobile phones are highly used for these considerations, there are still some constraints such as small storage space, low battery power and weak computing power. This is where mobile cloud computing comes into play, offering almost infinite storage space as well as access to computing resources.

Taking advantage of both mobile devices as well as cloud computing has given way to their integration on a single platform known as Mobile Cloud Computing (MCC). Thus, combining the advantages of cloud computing and mobile devices, a new paradigm is created. On the other hand, attribute based encryption is believed to be the best cryptographic primitives that is used in large scale distributed systems. However, the drawback with this encryption methodology is that it is not compatible with MCC. Hence in order to perform computationally intensive tasks, a typical mobile device will require an additional support or external resource. This is made possible by integrating mobile computing and cloud computing. The biggest worry with the use of MCC is consumer's concern about data privacy and safety when sensitive information is being outsourced.

2. Literature Survey

Over the years, numerous cryptographic primitives have been introduced, of which ABE was considered to be the most attractive one. This is mainly because of its ability to be identified as the public key for encryption. The Fuzzy identity-based encryption (IBE) was introduced by Sahai and Waters [1] in 2005. This was base for developing ABE and was considered to be its prototype. Similarly in [2], the authors further developed Fuzzy IBE to be used with attributes concept, leading to the development of ABE. Based on the ciphertext and secret key, ABE can be categorized into two types namely Ciphertext-Policy ABE [3] and Key-Policy ABE [2]. For the initial scheme, the access structure is associated with encrypted data and attributes are associated with user's secret key. Similarly in the latter scheme, set of attributes are related to the encrypted data and the access policy incorporates

ISSN: 2582-3167
Submitted: 19.12.2020
Accepted: 24.12.2020
Published: 02.01.2021

privacy keys of user [4]. Using ABE, a number of researches has been carried out in devising methods for secure data sharing successfully.

Despite ABE being most promising and powerful, they are still too expensive at pairing and are hence not an efficient option. However, in [6], Green et al. used an ABE methodology which makes use of a transformation key in an external cloud server. This ensures that the challenging operations that require more resources are done in the cloud server and smaller operations are performed by the mobile device. However, in order to reduce cost considerations, third-party untrusted decryption servers could be used, introducing semi-trust cloud server. In [7] Lai et al a methodology was introduced a methodology wherein outsourcing with guarantee of correction is performed. Similarly, a number of methods were further introduced in [8-10] using different ABE-based techniques with different properties.

3.Proposed Methodology

3.1 System Model

The ABE model for mobile cloud computing involves the use of 5 components namely Users, Owners, Mobile Cloud Computing (MCC), Cloud Service Provider (CSP) and Key Generation Center (KGC). The framework of the system and its communicating means using the ABE based outsourcing methodology is depicted in Fig.1. The following are the various parts of the system model and their role in the proposed approach:

- The owner refers to the mobile device users which have resource-constraint. However, when connected to a mobile computing cloud (MCC) these devices will be able to process the information in a more efficient manner.
- The mobile devices are integrated with the MCC to provide a powerful computing environment and seemingly infinite storage to ensure quick processing of data.
- Access and to decryption of the ciphertext lies in the hands of the Owner who holds the right to permit or deny.
- The message is produced and encrypted into ciphertext by the owner and then sent to the computer service provider to be stored and shared.
- A typical CSP is responsible for storing the data for the owner in an environment of semi-trust.
- Public and Private key pairs are generated and distributed by the KGC.

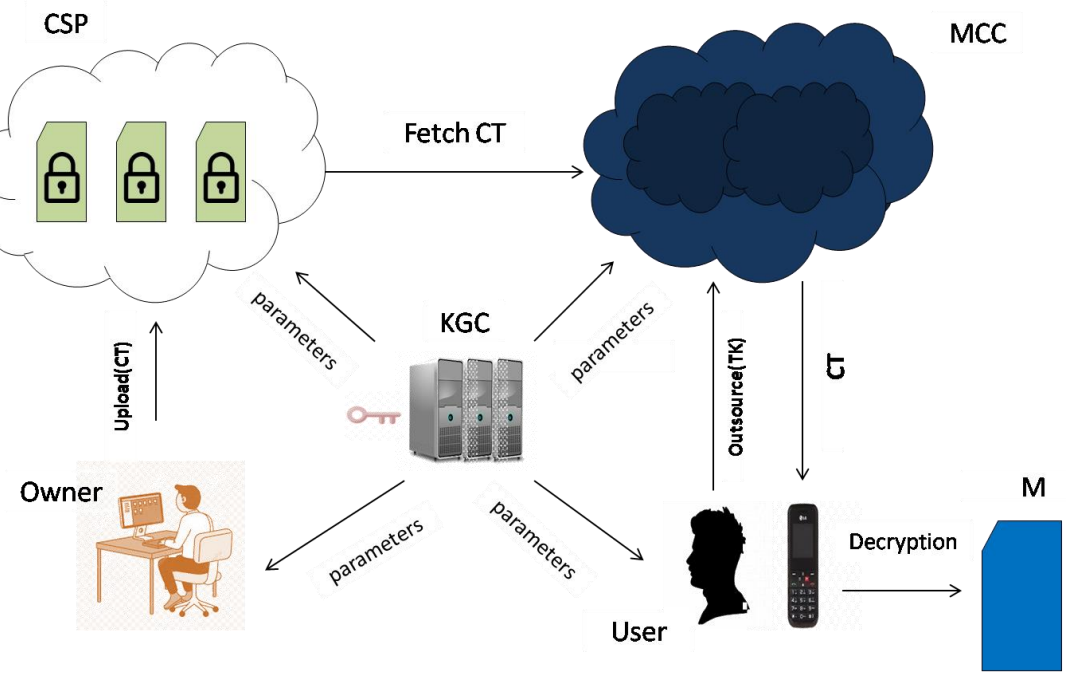

Fig.1. System Model of the Proposed Methodology

ISSN: 2582-3167
Submitted: 19.12.2020
Accepted: 24.12.2020
Published: 02.01.2021

3.2 Algorithms Implemented

In the proposed work, we have implemented 5 algorithms which are apt for using the MCC environment with ABE scheme in outsourcing. They are as follows:

1. Encrypt and Decrypt: Encryption is performed by the owner while decryption is performed by the user. At the owner side, the cipher text CT is produced by taking the message data along with access policy. Similarly, at the user end, with the key set, the ciphertext can be decrypted to retrieve the original message that was sent.
2. Setup: In order to initiate key generation, KGC will generate a master secret key along with public parameters.
3. Extract: Private key for the user in relationship with the attribute set is generated by KGC using attribute set, master secret key and public parameters.
4. Transform: The MCC makes use of the transformation key, the cipher text and public parameters to partially decrypt the output.
5. Output Decryption: The User will take the ciphertext and the public parameters to determine the message that was sent at the input, M.

3.3 Security

The mobile cloud computing methodology used is said to be semi-trust entity which indicates that there are possibilities that a third-party might have access to view the content of the encrypted data even though MCC is used perform its operation and provide the right results. In this section, we define a novel mode which enhances the security of MCC when an attacker tries to intercept the data. A challenging access structure is first declared by the attacker [11]. When the attacker attacks, there are two phases involved in rectifying the situation and identifying the attack. In face one three queries are issues namely decrypt query [12], key extraction query and output decryption query. In the next phase, there are two restrictions imposed on the attacker:

1. The attacker cannot make decryption query
2. The attacker cannot pick the right attribute set necessary to issue the private key query.

Hence at the end of the attack, the attacker's guess (let us consider it to be G') and the actual output (G) will prove to be true only if G'=G.

3.4 Proposed Concrete Construction

There are two bilinear cyclic groups that are used in setup process. They are used to hold a master key which remains a secret and public parameters are published. For a given set of attributes, a set of keys is generated by KGC, for the users. At the encryption front, the cipher text CT is created by calculating various specific parameters that are associated with individual nodes. At the user end, the received ciphertext is analyzed to find if the attribute set matches with access structure. If a match is hit, message from the cipher text can be further processed for decryption. On the other hand, if there is no match, the cipher text is immediately discarded without any further action. Using the MCC as the semi-trusted proxy, a transformation key is used in order to transform CT in a simpler cipher. A transformation between the MCC and the user is essential and the last step in the process is to use the transformation key to determine the actual message that was transmitted.

4. Results and Discussion

Using python programming on 64-bit processing Ubuntu platform, we have performed experimental simulation in Charm 0.43 software. We have conducted 40 simulations and the final result is taken to be the mean average of all the results obtained during simulation. Here Fig.2 represents comparison of the decryption that is outsourced with that of other non-decryption method. It is observed that as the number of attributes begin to increase, the decryption time taken also increases simultaneously, in a rapid fashion.

ISSN: 2582-3167
Submitted: 19.12.2020
Accepted: 24.12.2020
Published: 02.01.2021

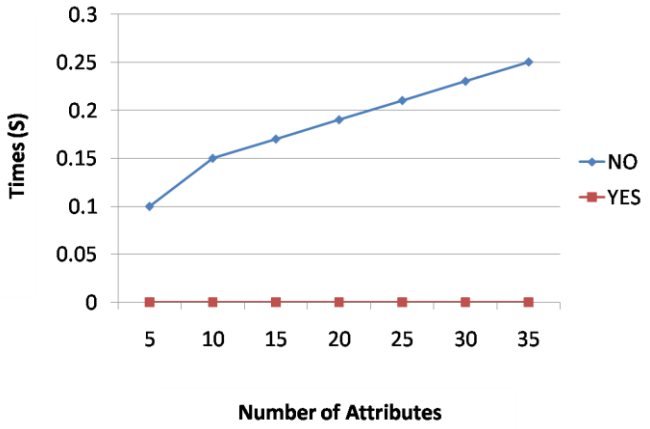

Fig.2 Outsourced Decryption VS. Non-Outsourced Decryption

Fig.3 depicts a comparison of the decryption time for the outsourced data between our proposed scheme, Fan et al.'s [14] scheme and Lai et al.'s [13] scheme. It is observed that our scheme outperforms that of Lai et al.

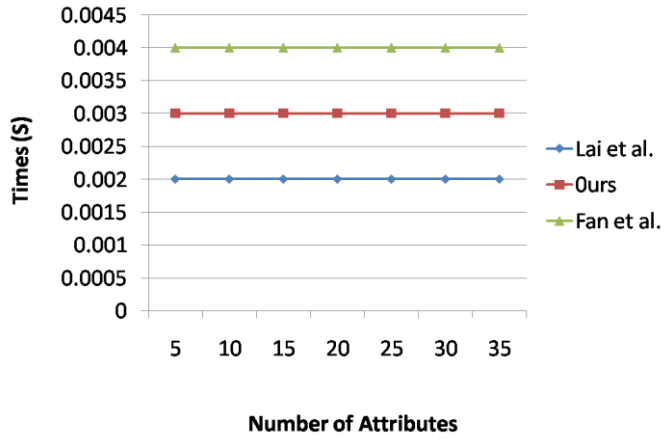

Fig.3. Decryption Time for Outsourced Methodology

5. Conclusion

In this proposed methodology, we have implemented a novel ABE enforced Mobile cloud computing which is considered to be a secure means of data exchange. This method supports security properties such as achieving CCA security level, preventing decryption key exposure and checkability. In this methodology we have made use of a transformation key in order to make use of resources on the cloud for operations that are considered to be time consuming. Performance analysis and security results indicate that this method is very practical and highly secure to be used with mobile cloud computing. Future work will involve ABE schemes which are developed with post-quantum security in order to prevent or fight against attacks from quantum computers, in the future.

References

[1] Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.

[2] 13. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 30 October–3 November 2006; pp. 89–98.

[3] 14. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE symposium on security and privacy (SP'07), Berkeley, CA, USA, 20–23 May 2007; pp. 321–334.

ISSN: 2582-3167
Submitted: 19.12.2020
Accepted: 24.12.2020
Published: 02.01.2021

[4] Suma, V., & Hills, S. M. (2020). Resource Intensification for Mobile Devices Using the Approximate Computing Entities. Journal of trends in Computer Science and Smart technology (TCSST), 2(01), 26-36.
[5] Haoxiang, W., & Smys, S. (2020). Secure and Optimized Cloud-Based Cyber-Physical Systems with Memory-Aware Scheduling Scheme. Journal of trends in Computer Science and Smart technology (TCSST), 2(03), 141-147.
[6] Green, M.; Hohenberger, S.; Waters, B. Outsourcing the decryption of abe ciphertexts. In USENIX Security Symposium; USENIX Association: San Francisco, CA, USA, 2011; pp. 1–16. 26.
[7] Lai, J.; Deng, R.H.; Guan, C.; Weng, J. Attribute-based encryption with verifiable outsourced decryption. IEEE Trans. Inf. Forensics Secur. 2013, 8, 1343–1354.
[8] Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., & Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Journal of Information Security and Applications, 55, 102582.
[9] Mo, J., Hu, Z., Chen, H., & Shen, W. (2019). An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing. Wireless Communications and Mobile Computing, 2019.
[10] Munivel, E., & Kannammal, A. (2019). New authentication scheme to secure against the phishing attack in the mobile cloud computing. Security and Communication Networks, 2019.
[11] Chaudhry, S. A., Kim, I. L., Rho, S., Farash, M. S., & Shon, T. (2019). An improved anonymous authentication scheme for distributed mobile cloud computing services. Cluster Computing, 22(1), 1595-1609.
[12] Muneera, B. H., Janeera, D. A., Shankar, B. M., & Ruth Anita Shirley, D. (2020, September). Edge Preserving Filter Selection for Noise Removal and Histogram Equalization. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 567-571). IEEE.
[13] Lai, J.; Deng, R.H.; Guan, C.; Weng, J. Attribute-based encryption with verifiable outsourced decryption. IEEE Trans. Inf. Forensics Secur. 2013, 8, 1343–1354.
[14] Fan, K.; Liu, T.; Zhang, K.; Li, H.; Yang, Y. A secure and efficient outsourced computation on data sharing scheme for privacy computing. J. Parallel Distrib. Comput. 2020, 135, 169–176.
[15] Yang, Y.; Liu, X.; Deng, R.H.; Li, Y. Lightweight sharable and traceable secure mobile health system. IEEE Trans. Dependable Secur. Comput. 2020, 17, 78–91.

ISSN: 2582-3167
Submitted: 19.12.2020
Accepted: 24.12.2020
Published: 02.01.2021