WOAS WORLD ORGANIZATION OF APPLIED SCIENCES JOURNALS

International Journal of Information Technology and Applied Sciences
ISSN (2709-2208)
Int. J. Inf. Tec. App. Sci. 3, No.1 (Jan-2021)
https://doi.org/10.52502/ijitas.v3i1.15

# Proposal for a Secure Data Sharing and Processing in Cloud Applications for Healthcare Domain

**Mbarek Marwan, Ali Karti and Hassan Ouahmane**
*Chouaïb Doukkali University, Laboratory LTI, Department TRI, ENSAJ, El Jadida, Morocco*

**Abstract:** Information Technology (IT) services have become an inherent component in almost all sectors. Similarly, the health sector has been recently integrating IT to meet the growing demand for medical data exchange and storage. Currently, cloud has become a real hosting alternative for traditional on-permise software. In this model, not only do health organizations have access to a wide range of services but most importantly they are charged based on the usage of these cloud applications. However, especially in the healthcare domain, cloud computing deems challenging as to the sensitivity of health data. This work aims at improving access to medical data and securely sharing them across healthcare professionals, allowing real-time collaboration. From these perspectives, they propose a hybrid cryptosystem based on AES and Paillier to prevent the disclosure of confidential data, as well as computing encrypted data. Unlike most other solutions, the proposed framework adopts a proxy-based architecture to tackle some issues regarding privacy concerns and access control. Subsequently, this system typically guarantees that only authorized users can view or use specific resources in a computing environment. To this aim, they use eXtensible Access Control Markup Language (XACML) standard to properly design and manage access control policies. In this study, they opt for the (Abbreviated Language for Authorization) ALFA tool to easily formulate XACML policies and define complex rules. The simulation results show that the proposal offers simple and efficient mechanisms for a secure use of cloud services within healthcare domain. Consequently, this framework is an appropriate method to support collaboration among all entities involved in medical information exchange.

**Keywords:** Cloud computing, medical data, security, access control.



## 1. INTRODUCTION

Cloud applications aim at significantly reducing costs while generally delivering high service quality. Thus, healthcare organizations are interested in using cloud-based electronic health systems to manage and share patients' data. The most important feature of using cloud services is that it lets clients outsource both the storage and computations to an external entity. This would inevitably lead to a reduction in operating costs and better productivity. Indeed, the cloud provider is responsible for the maintenance and upgrade of the delivered cloud services so as healthcare professionals focus on their core activities. More interestingly, the basic pricing scheme in this paradigm follows a pay-per-use model and Service Level Agreement (SLA) to meet user's demands [1]. This new paradigm has received peculiar attention from both the healthcare industry and academic community as an affordable alternative to traditional on-premises software. Although these efforts can certainly lead to satisfactory outcomes, outsourcing IT services to third-party service providers may raise significant challenges [2].

In particular, the usage of this technology in the healthcare domain can seriously pose security and privacy problems. In light of these facts, we explore the most frequently encountered threats associated with cloud computing and examine the root causes of security risks. Usually, clients have limited capability to manage their data since their data are often processed and stored on off-site servers. This situation negatively impacts the desirable level of protection for medical data. We strongly recommend that data security should be addressed before migrating to cloud computing.

The most obvious approach to this issue is to simply encrypt clients' data before sending them to cloud providers to maintain confidentiality. Unfortunately, such an assumption does not always seem practical given the complexity of managing encrypted data. In other words, cloud providers are not able to process outsourced data if they do not have the secret decryption key. Additionally, the security of medical data is naturally of the utmost importance in the healthcare sector because these data play a crucial role in diagnosis and further analysis. Therefore, healthcare organizations put a heavy emphasis on privacy and security when using cloud services. In this regard, we propose a secure framework to easily store, retrieve, and manage health records. Meanwhile, the proposal is a simple collaboration system to share medical data and improve interoperability among diverse healthcare information systems. For example, cloud providers offer online applications to manage and share personal health information (PHI) easily and in real-time. Technically, these remote resources are accessible through

web interfaces or specific APIs. Accordingly, it enables data exchange among healthcare ecosystems, namely radiology centers, hospitals, insurance companies, and patients.

In such a concept, doctors can have access to these remote cloud applications to manage medical data and retain health information. Moreover, company insurances rely on this framework to scrutinize patients' transactions and to view all care received by a patient from multiple care delivery organizations. In this case, reducing frauds and improving healthcare quality are the main tangible benefits gained through effective interprofessional collaboration and teamwork in the healthcare domain. One of the major aspects offered by leveraging cloud services is the possibility to access health records anywhere and anytime, as well as facilitating the ability to share medical information. However, privacy issues in this model are some of the biggest concerns surrounding the adoption of cloud technology in the healthcare domain. To overcome these challenges and comply with the law, we develop a framework that offers a number of benefits and services to both consumers and cloud providers. First, we suggest a hybrid approach to protect the privacy of medical information and enforce confidentiality while processing data. In fact, the suggested cryptosystem is designed to protect medical information and allow computations on encrypted data. Second, we use XACML standard for modeling and implementing security policies. To this end, we rely on ALFA tool to develop a system that ensures identity and access management, thereby automatically providing access restriction.

The rest of this paper is organized as follows. Section II gives a concise description of the current frameworks. Section III, we describe the proposed model that meets privacy requirements. Section IV highlights the main security measures to mitigate security threats. In Section V, we implement our solution to prove its correctness. Finally, Section VI gives some concluding remarks and outlines opportunities for future research.

## 2. Related Work

This section aims at providing some important contributions from the existing implementations, as well as briefly outlining different security mechanisms. In [3], Zhao et al. propose a Progressive Elliptic Curve Encryption (PECE) [13] scheme to ensure data security in cloud environment. Subsequently, the secret data are often encrypted many times using several keys. The decryption function is designed in such an approach that the owner uses only one key. In this case, clients should encrypt their data through the use of their private keys. Afterward, the data owner sends a credential to a third-party provider to encrypt confidential data so that the owner can share them with authorized users. For simplicity, the same credential will typically enable authorized users to perform decryption operations. Although this method ensures secure data sharing, it has certain limitations regarding encryption key management. In fact, according to this model, the owner should know the private key of the cloud provider.

Samanthula et al. [4] suggest security measures to protect data and prevent unauthorized disclosure. More specifically, they use homomorphic algorithms and proxy re-encryption model to meet privacy requirements. One of the most important practical benefits is the ability to carry out arithmetic operations on ciphertexts. In other words, it is possible to outsource computations to an external party without revealing the secret data. Since homomorphic encryptions are time-consuming algorithms, this solution has serious drawbacks as to the system performance, despite its remarkable ability to safeguard personal data. Wang et al. [5] develop a proxy re-encryption solution to ensure security in a collaborative environment. In such a scheme, clients encrypt their sensitive data using the public keys for secure data sharing. Afterward, they send ciphertexts to a semi-trusted proxy. The latter is able to transform the ciphertext into another format without learning the underlying plaintext. At the same time, only authorized users can decrypt data by using their private keys.

Gondkar et al. [6] suggest an efficient approach based on Attribute-Based Encryption (ABE) to protect personal health information. More specifically, Multi Authority ABE (MAABE) is used to maintain the confidentiality of clients' data. In particular, this technique is most appropriate in creating a collaborative environment and sharing data. In fact, it allows dynamic modification of access policies for fine grained rights management.

Ibraimi et al. [7] propose a framework to secure medical data. They rely on ciphertext policy ABE (CP-ABE) mechanism to manage and share medical data. More importantly, the concept of social professional domains is applied in this specific situation instead of multi-authority ABE. Consequently, the proposal provides required security and appropriate standards for managing and sharing health records.

## 3. Proposed Framework

Broadly speaking, Security issues in cloud computing are heavily contingent on the preventive uptake of complex measures which are required to be at least at the same level of the possible threats if not anticipating more challenging ones. The literature review reveals that there are a number of diverse factors influencing customer satisfaction and trust in cloud computing. In light of this fact, robust security measures are required to make sure that internal or external users cannot reach confidential medical data. More importantly, the proposed techniques should offer the appropriate level of data protection and allow cloud providers to perform computations on ciphertexts. To deal with these challenges, we propose a hybrid approach based on two known cryptosystems which take advantage of both the traditional strong cipher and the homomorphic approach. In an effort to better

respect privacy policy rules, our framework relies on an access control system to avoid data disclosure. Consequently, the proposed framework is meant to provide two basic services to clients, i.e., data protection and access control.

### A. Proposed Approach

With the advent of cloud, the utilization of online services in the healthcare sector has dramatically grown in the past few years. This model provides powerful tools to increase cooperation among healthcare providers, facilitate sharing of medical data, and enhance processing capabilities. Thus, cloud technology has brought changes to every corner of the healthcare sector. In this context, the proposed solution is built on off-site servers to boost the exchange of medical data among clients. Subsequently, this application is designed to help healthcare professionals view and manage patient's medical records. Undoubtedly, it is an efficient collaborative healthcare solution, providing rapid access to personal medical records. Despite all these advantages, cloud services are developed without careful considerations of privacy compliance in the healthcare context. To address these issues, we design and develop a cloud framework to meet the required standards of security and privacy. In this case, we propose a hybrid cryptosystem to meet healthcare organization's needs, security policies, and compliance with laws and regulations. Particularly, in this proposed framework, we use an hybrid approach based on Advanced Encryption Standard (AES) and Paillier cryptosystem [8] to safeguard patients' medical data. The most efficient way to manage the distribution of encryption keys is by using the asymmetric encryption algorithm RSA [14]. In order to apply this cryptosystem, each client has normally two keys referred to as public and private keys.

As regards enforcement of security interest, we introduce a third party called CloudSec that principally provides security mechanisms as a service. In this case, this entity ensures two main functions: data encryption and encryption key management, as shown in Fig. 1.

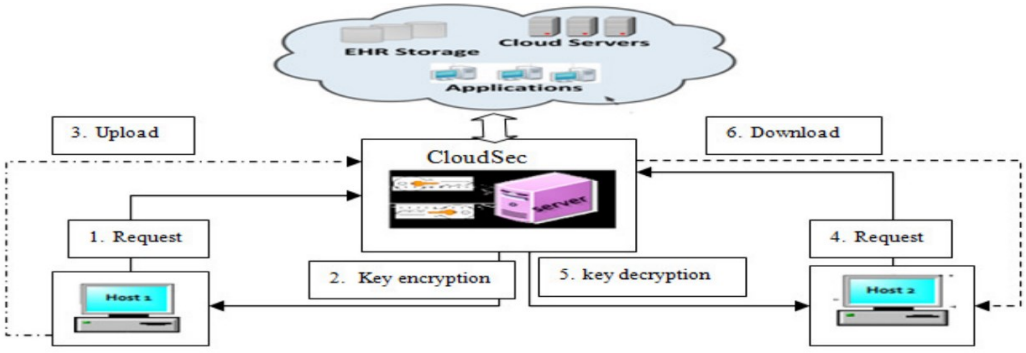


Fig. 1. Overview of the proposed architecture.

In practice, a web-based interface typically provides all required security methods and mechanisms to help healthcare organizations manage their medical data easily and efficiently. In this framework, CloudSec module relies on security policy to examine and determine who is authorized to access cloud resources. In order to grant or revoke permission to perform an operation, it is highly important for an organization to select the appropriate access control model. Today, there exists a wide range of access control models with different mechanisms for protecting data from unauthorized access, use, and disclosure. The most famous existing products for protecting shared resources include Discretionary Access Control (DAC) [15], Mandatory access control (MAC) [16], Role-based access control (RBAC) [17], Attribute-Based Access Control (ABAC) [18]. When examining available solutions, it has been found that ABAC is specifically tailored to the needs of cloud environment [9]. Another important aspect is that this model evaluates rules against the attributes of the entities (subject and object) through the use of security policy. This evidence shows the importance of security policy to list all of the permitted and prohibited operations more efficiently. Consequently, the proposed framework provides a secure application to share and manage patients' medical information over cloud computing. More importantly, healthcare professionals can use and access remote cloud-based services through the Internet both safely and instantly.

In this work, we mainly focus on data confidentiality using both AES and a homomorphic scheme. Besides, the proposal offers access control as a service to reinforce data privacy. After we define precisely a security policy, we use XACML [19] (eXtensible Access Control Markup Language) to process the authorization requests according to policy rules.

### B. The proposed secure data management approach

In this work, we propose a hybrid solution to address the security issues in cloud computing during data storage and processing. More precisely, this technique is inspired by multilevel security approach in which data are

classified into different categories according to their significance and sensitivity levels. Subsequently, medical data are divided into two classes: patient's identifying information and numerical data. In this sense, the first type of data is encrypted using Advanced Encryption Standard (AES) [20] to prevent data disclosure. Alternatively, we use Pallier algorithm to encrypt other data at the following stage to reinforce the security. Mainly, the second algorithm aims at performing mathematical operations on encrypted data, since it is an additive homomorphic cryptosystem.

As regards the system architecture, we propose CloudSec as a trusted third party that provides secure API's. In other words, this core entity provides an interface between clients and cloud providers. Therefore, this module aims at reducing security risks when moving to cloud computing and helping cloud providers to restrict access, detect abuse and prevent any data misuse. The primary responsibility of protecting personal health information in this framework lies with CloudSec which acts as a proxy system. In essence, this component encrypts the patient's identifying information such as name, social security number (SSN), care organization, and type of medical service. These usually involve an algorithm used in symmetric key cryptography, i.g., Advanced Encryption Standard (AES). Meanwhile, the numerical data are encrypted through a homomorphic cryptosystem, i.g., Paillier algorithm. Based on these measures, all medical data are encrypted using a hybrid cryptosystem before transmitting them to the cloud computing. Another important point is that CloudSec stores metadata such as SSN, search keywords and encryption keys (Akey for AES and Pbkey, PrKey for public and private Paillier keys) in a secure local database called MasterIndex.

Functionally, CloudSec sends a request to the public cloud for accessing and performing operations on remote healthcare applications. For instance, the proposed solution enables to perform homomorphic addition of medical costs. Therefore, in order to locate a patient's record, the CloudSec uses a keyword to get exact matching results of the client's request. In this case, cloud provider returns the results of the original request in encrypted form to preserve data privacy. Finally, the CloudSec has to decrypt data using its private key to get the final results and then sends a response back to the healthcare organization. We present an example of a specific case illustrating the most significant interactions when CloudSec sends data to the cloud provider, as shown in Fig. 2.

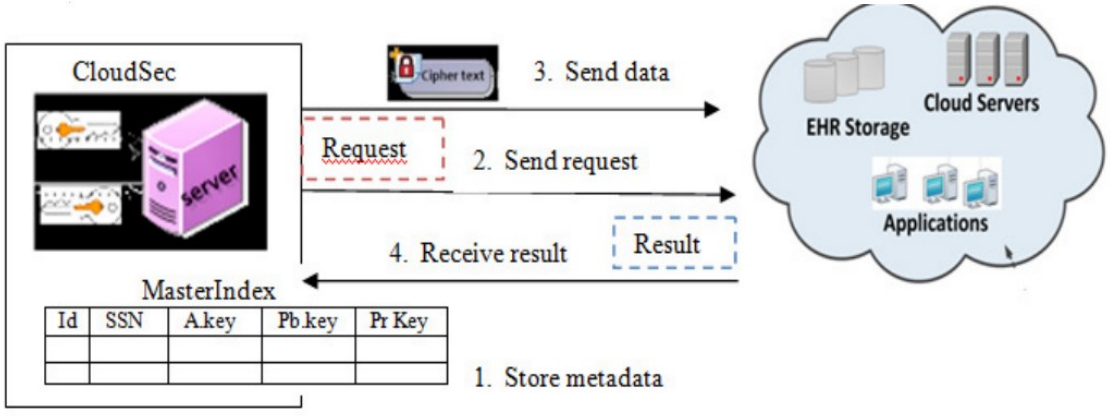


Fig. 2. Communication between CloudSec and cloud computing.

In short, the necessary mechanism to achieve the confidentiality goal is based on two main types of encryption algorithms: (1) Paillier algorithm to encrypt medical costs, (2) AES algorithm to cipher other patient's medical information. Thus, we use Algorithm 1 in order to tackle the privacy issues faced in cloud solutions. Of course, CloudSec uses encryption keys to produce ciphertexts that are secure against unauthorized access and use.

**Algorithm 1.** EncryptData

1: Input: D, SSN, where D is medical data, SSN is social security number; A refers to AES Algorithm, and P to Paillier Algorithm
2: Output: < C > if SSN exist in MasterIndex database
3: Akey ←MasterIndex [SSN]
4: PrKey ←MasterIndex [SSN] \\Retrieve encryption keys form the MasterIndex database
5: PbKey ←MasterIndex [SSN]
6: else
7: Akey←genaratekey (AES) \\ Generate encryption keys
8: {PrKey, PbKey} ←generateKey (Paillier)
9: Save_in_MasterIndex (SSN, AKey, PrKey, PbKey)
10: if D is numerical data
11: then C←Paillier (m, Pbkey)
12: else
13: C←A (m, Akey)
14: endif
15: return

In practice, these keys are either already stored in the MasterIndex database or newly generated. For technical reasons, we use Social Security Number (SSN) to easily

create encryption keys that perform encryption and decryption.

## 4. Background on The Proposed Methods

Cloud computing has completely shifted the way healthcare organizations use IT services to improve patient care. However, this new paradigm faces several problems related to security, privacy and trust concerns. Regardless of the cloud delivery model, it is necessary to rigorously address these issues in order to ensure a successful cloud deployment. In this context, the main challenges are linked to the fact that this technology is typically controlled by a third-party service provider. In this respect, we propose cryptographic techniques and XACML-based access control model to deal with threats and vulnerabilities associated with cloud computing. By leveraging these techniques, the proposal ensures the protection of cloud services so that only the authorized clients are granted access to or view medical data. In this section, we present the two used cryptosystems and the proposed access control model.

### A. Paillier Algorithm

Originally, homomorphic algorithms are developed in such a way that one can compute encrypted data. By leveraging these techniques, we can operate the ciphertext of two values to get the encrypted result which, when decrypted, matches the result of the operation associated with these two values in plaintext form. Among these cryptosystems, the paillier algorithm is one of the most widely used techniques to handle encrypted data. More specifically, it is a probabilistic asymmetric algorithm and used to support additive homomorphic operations over encrypted data. In this scheme, we first need to generate public and private keys. We then can encrypt and decrypt the private data for privacy protection, as shown in Algorithm 2 [8].

**Algorithm 2.** Paillier cryptosystem

**Input:** $m \in \mathbb{Z}_n$
**Output:** $c \in \mathbb{Z}_n^2$
**Function KeyGeneration (p, q)**
Setp 1: Select two p, $q \in \mathbb{P}$
Step 2: Compute n=p.q
Step 3: Select $g \in \mathbb{Z}^*_{n_2}$ in such a way that n and L ($g^\lambda \bmod n^2$) are coprime, gcd (L (L($g^\lambda \bmod n^2$)), n) =1, with L(u) = $\frac{u-1}{n}$
Step 4: Create keys
Public key: pk = (n, g)
Secret key: sk = (p, q)
**Function encryption Enc (m, pk)**
Step 1: Choose $r \in \mathbb{Z}^*_n$
Step 2: Compute $c = g^m r^n \bmod n^2$
**Function decryption Dec(c, sk)**
Compute $m = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$

### B. The proposed access control model

Access control is one of the key measures we need to implement in order to ensure data protection. In this context, CloudSec offers required mechanisms to limit access to specific data in a remote cloud database, thereby providing access control as a service. Broadly speaking, there currently exist various approaches for restricting access to specific resources, software, and system. Among them, MAC, DAC, RBAC and ABAC are commonly used as systems of access control in a shared resource environment.

In many cases, these traditional models are often not designed to support the access control in an untrusted, distributed domain like cloud computing. In this respect, we propose an efficient solution that ensures that authorization decisions will be made in accordance with the security policy. Fig. 3 provides an overview of the basic principles of the proposed system to provide access control in cloudbased applications.

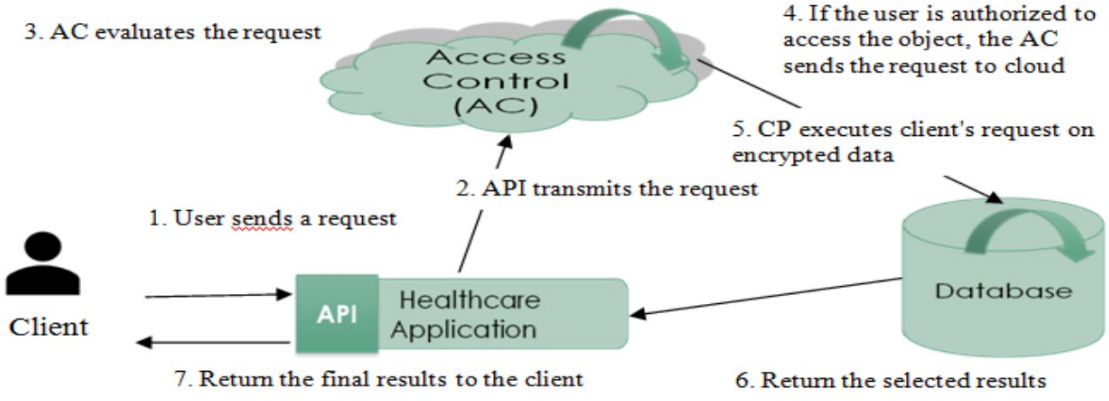


Fig. 3. Principle of access control mechanism.

To reinforce data security, we use XACML 3.0 [10,11] (OASIS) to implement a security policy. In this study, we use Abbreviated Language for Authorization (ALFA) [12] Eclipse plugin to facilitate the formulation and expression of access-control policies. In this respect, we use the free open source to write an ALFA policy instead of using traditional XACML. More importantly, this tool allows users to represent the domain specific information, especially rules, attributes, and policy. Additionally, ALFA policy is an efficient tool to ensure the security of the developed application. Based on these considerations, we first define cloud_application as a namespace of the ALFA policy. Second, we use policy.alfa as a security policy that contains a set of authorization rules and restrictions to medical information. Third, we define medicalInformation as a policyset and medicalRecordAccess as a policy. By default, the standard plugin contains standardattributes.alfa and system.alfa files, which typically define rules and attributes. Here, the pseudo-code that can be used to write fine-grained authorization policies using the ALFA policy.

```
namespace cloud_application {
policyset medicalInformation { apply
permitOverrides
medicalRecordAcces }
policy medicalRecordAcces { target clause
Attributes.resourceType == “medical record”
apply denyOverrides rule { permit target clause
Attributes.role == “doctor” }
rule controlUser { deny condition
not(booleanOneAndOnly(Attributes.careRelationEx
ist s))
on deny { advice ObligationAdvice.reasonForDeny
{
Attributes.message = “There is no care
relation” }
}
}
rule permitEditdoctors { target clause
userType=="doctor" and actionId=="edit" permit
}
rule RecordAvailability { deny Condition
booleanOneAndOnly(Attributes.recordIsBlocked) }
rule permitViewdoctors { target clause
userType=="doctor" and actionId=="view"
permit } } }
}
}
```

Concretely, we define four rules to enhance patients' privacy and ensure data protection against unauthorized access. In practical security terms, a higher level of privacy protection can be achieved through the implementation of a security policy. More specifically, this policy enables doctors, in this case, to view and edit medical records. Simultaneously, it blocks doctors who do not have a caregiving relationship to the patient.

## 5. Simulation Results

Protecting sensitive data when using cloud computing is the end goal of the proposed solution. In this respect, we use AES to saveguard patients' information and Pallier to encrypt numerical data. In this context, the algorithms were coded in JAVA programming language [21]. Besides, we use MySQL [22] as a database to build the proposed healthcare application. For security reasons, the authentication is commonly done through a login dialog where users can manually enter their username and password. After entering valid credentials, users can connect to the database and access specific tables and views according to the security policy, as presented in Fig. 4.




Fig. 4. Medical data in plaintext form.

As outlined above, there are serious security problems in cloud computing, which can expose sensitive data to potential disclosure risks. The nature of cloud computing makes it difficult to prevent all insider attacks. Moreover, clients have less control over their data since cloud provider is entirely responsible for data management. In

this regard, we should encrypt all data before uploading them to the cloud servers in order to make sure that medical information remains safe from both internal and external users. More specifically, we use AES and Paillier algorithms to encrypt all data stored in the cloud to meet privacy requirements, as shown in Fig. 5.


Fig. 5. Encrypted medical information.

Concerning other services, the proposed application offers the possibility to compute encrypted data. In particular, the Paillier algorithm is used to support additional operations on ciphertexts. By leveraging this method, we can calculate the total medical costs of a specific client in total security and confidentiality. As a matter of illustration, we apply this method to estimate total costs for user = marwan. After the successful completion of the decryption process, we obtain the result 900, as shown in Fig. 6. More interestingly, this result is equal to the sum of two numbers 400 and 500.


Fig. 6. The addition of two encrypted values.

## 6. Conclusion and Future Work

As regards effectiveness, cloud services can play a significant role in the management and exchange of medical information. However, the security component is one of the most important concerns that require meticulous attention when outsourcing IT services. In this respect, appropriate strong security mechanisms are required to handle specific situations in which sensitive personal data are stored in remote cloud servers. Thanks to encryptions techniques, cloud providers can protect the consumers' data against unauthorized use and disclosure. Unfortunately, these traditional cryptographic methods are not able to perform properly mathematical operations on encrypted data. To overcome this challenge, we use a hybrid approach to use cloud applications in the most efficient and safe possible way. More precisely, we use AES and Paillier to achieve a high level of security for cloud applications. Based on these considerations, we rely on homomorphic encryption to encrypt numerical data, while the other data are encrypted using AES. Additionally, we use an access control system to ensure that only authorized users gain access and view medical information stored in a cloud database. To this aim, we use XACML language to express security policies and access rights. For the purpose of simplicity, we use ALFA policy to facilitate the implementation of appropriate security policies. The results of the simulation prove the accuracy and correctness of the proposed solution for data protection. Consequently, this framework could help clients minimize security risks in the cloud computing; thereby, promoting this concept in the healthcare domain. In future work, we intend to explore the possible utilization of fully homomorphic encryption in order to execute requests involving complex processing functions. Moreover, we will design and configure a robust and flexible access control model by using both Attribute-based Access Control (ABAC) and XACML policy language.

## REFERENCES


[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Technical Report, National Institute of Standards and Technology, vol. 15, 2009, pp. 1-3.

[2] Qian, L., Z. Luo, Y. Du and L. Guo, "Cloud Computing: An Overview," The 1st International Conference on Cloud Computing (Beijing, China), pp. 626–631, 2009.

[3] Zhao, G., C. Rong, J. Li, F. Zhang and Y. Tang, "Trusted Data Sharing Over Untrusted Cloud Storage Providers," International Conference on Cloud computing Technology and Science (CloudCom), pp. 97–103, 2010.

[4] Samanthula, B., G. Howser, Y. Elmehdwi and S. Madria, "An Efficient and Secure Data Sharing Framework using Homomorphic Encryption in the Cloud," International Workshop on Cloud Intelligence (Cloud-I '12), Vol. 8:1-8, 2012.

[5] Wang X. and W. Zhong, "A New Identity Based Proxy Re-encryption Scheme," International Conference on Biomedical Engineering and Computer Science (ICBECS), pp. 145–153, 2010.

[6] Gondkar, D.A. and V.S. Kadam. "Attribute Based Encryption for Securing Personal Health Record on Cloud," International Conference on Devices, Circuits and Systems (ICDCS), pp.1-5, 2014.

[7] Ibraimi, L., M. Petkovic, S. Nikova, P. Hartel and W. Jonker, "Ciphertext Policy Attribute Based Threshold Decryption With Flexible Delegation and Revocation of User Attributes," Technical Report, 2009. [Online]. available: https://research.utwente.nl/files/5098396/Technical_Report.pdf

[8] Paillier, P., "Public-key Cryptosystems Based on Composite Degree Residuosity Classes," International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'99), Springer, Berlin, Heidelberg, pp. 223–238, 1999.

[9] Ed-Daibouni, M., A. Lebbat, S. Tallal and H. Medromi, "Toward a New Extension of The Access Control Model ABAC for Cloud Computing," Lecture Notes in Electrical Engineering, Advances in Ubiquitous Networking, Springer, Vol. 366, pp 79-89, 2016.

[10] OASIS, "eXtensible Access Control Markup Language (XACML) version 3.0," [Online] Available at

[11] Bertolino, A., F. Lonetti and E. Marchetti, "Systematic XACML Request Generation for Testing Purposes," IEEE International Conference on Software Engineering and Advanced Applications (SEAA), pp. 3–11, 2010.

[12] Axiomatics, "Axiomatics Language for Authorization (ALFA)," [Online] Available at: http://www.axiomatics.com/axiomatics-alfa-plugin-for-eclipse.html. [Accessed 26 Jan. 2018].

[13] Zhao, G., Rong, C., Li, J., Zhang, F., & Tang, Y. (2010, November). Trusted Data Sharing over Untrusted Cloud Storage Providers. In CloudCom (pp. 97-103).

[14] Farah, S., Javed, Y., Shamim, A., & Nawaz, T. (2012, December). An experimental study on performance evaluation of asymmetric encryption algorithms. In Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science,(EECS-12) (pp. 121-124).

[15] Sandhu, R., & Munawer, Q. (1998, October). How to do discretionary access control using roles. In Proceedings of the third ACM workshop on Role-based access control (pp. 47-54).

[16] Osborn, S. (1997, November). Mandatory access control and role-based access control revisited. In Proceedings of the second ACM workshop on Role-based access control (pp. 31-40).

[17] Ferraiolo, D., Cugini, J., & Kuhn, D. R. (1995, December). Role-based access control (RBAC): Features and motivations. In Proceedings of 11th annual computer security application conference (pp. 241-48).

[18] Hu, V. C., Kuhn, D. R., Ferraiolo, D. F., & Voas, J. (2015). Attribute-based access control. Computer, 48(2), 85-88.

[19] Ramli, C. D. P. K., Nielson, H. R., & Nielson, F. (2014). The logic of XACML. Science of Computer Programming, 83, 80-105.

[20] Heron, S. (2009). Advanced encryption standard (AES). Network Security, 2009(12), 8-12.

[21] Arnold, K., & Gosling, J. (2005). The Java programming language.

[22] MySQL, A. B. (2001). MySQL.