IOP Conf. Series: Materials Science and Engineering **263** (2017) 042080 doi:10.1088/1757-899X/263/4/042080

Supporting reputation based trust management enhancing security layer for cloud service models

Karthiga.R , M.Vanitha, I. Sumaiya Thaseen and Mangaiyarkarasi. R

School of Information Technology and Engineering, VIT University, Vellore, India.

Email: mvanitha@vit.ac.in

Abstract. In the existing system trust between cloud providers and consumers is inadequate to establish the service level agreement though the consumer's response is good cause to assess the overall reliability of cloud services. Investigators recognized the significance of trust can be managed and security can be provided based on feedback collected from participant. In this work a face recognition system that helps to identify the user effectively. So we use an image comparison algorithm where the user face is captured during registration time and get stored in database. With that original image we compare it with the sample image that is already stored in database. If both the image get matched then the users are identified effectively. When the confidential data are subcontracted to the cloud, data holders will become worried about the confidentiality of their data in the cloud. Encrypting the data before subcontracting has been regarded as the important resources of keeping user data privacy beside the cloud server. So in order to keep the data secure we use an AES algorithm. Symmetric-key algorithms practice a shared key concept, keeping data secret requires keeping this key secret. So only the user with private key can decrypt data.

Key Terms - face recognition, trust management service (TMS), security, credentials.

1. Introduction

Cloud security refers to the set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of cloud computing. Every enterprise will have its own identity management system to control access to information and computing resources. However, privacy has been continued as main hurdle preventing the acceptance of cloud computing by a broader range of users applications. A number of safety threats are related with cloud data services. Two main concerns for the users of cloud are security and privacy of data. The issue is serious as the data is located in different places across the globe. Hence an asymmetric AES algorithm is used for securing the data. An efficient reliable and user authentication and data protection is utilized to secure the service. A face recognition system is utilized to authenticate the user and AES has been used as symmetric cryptographic algorithm for securing the data.

2. Related Work

Talal H.Noor [1] proposed supporting reputation based trust management that enhances security layer for cloud services. In the existing works trust between cloud providers and consumers is inadequate to establish the service level agreement. Investigators have identified that the implication of trust can be managed and security can be provided based on feedbacks collected from participants. Disadvantage here is that the accessibility of TMS is a problem because of unpredictable count of users and the extremely active nature of the cloud environment. Misleading feedback increase the trust result of cloud services. Multiple identities are used to distinguish the negative historical records. Identification security is the most important and difficulties for the cloud deployment. Many works to overcome the issue of image comparison algorithm where the user face is captured during registration time and get stored in database. With that original image we compare it with the sample image that is already stored in database. If both the image get matched then the users are identified effectively. Advantage include keep the users can be identified effectively, keeps data secure, high response time. Sheikh Mahbub Habib [1] proposed the challenges in the cloud computing environment and discussed about the trust and the reputation of their proposed system. In this the authors has discussed the ways to evaluate the quality of the service for the vendors on the basis of elasticity, response time and availability. So the proposed work on a trust and reputation systems to determine this service in inter cloud computing environment. Qiang Guo [3] introduced Modeling technology and also the evaluation of trust ratio in the cloud environments. The author has used the ETEC (Extensible trust Evaluation model for cloud computing environment to calculate the trust with a time variant. So they proposed a trust degree evaluation method which is used to calculates the various trust factors such as direct trust and indirect trust so it could be provided a**n** extent to improve the fault tolerance, robustness and the security of cloud system.

Aiiad Albeshri [3] proposed an idea of Mutual security of data in a Cloud computing environment. This paper provides the web services viewpoint and it does not cover many issues in security. They proposed an opposite access control so the customers are controlled and authenticated within the cloud computing environment. Zheng Yan[5] proposed a data access control created on trust in cloud environment. The author used the access control list and role based access control which doesn't support data accesses flexibly. So, In this paper multidimensional controlling of cloud data is proposed which is based on the rules fixed by the data holders. We mainly provide security for the data by controlling its access based on the trust and reputation evaluated by data owner. Sebastian Ries [6] introduced Towards Trust Management System for Cloud Computing .The author has considered the service level agreement as a agreement among user and cloud service provider where the service level agreement were not standardized for the stakeholders in the cloud environment. They proposed a multi faceted system architecture for trust management. This system helps to identify the reliable cloud environment in terms of dissimilar attributes.

Hassan Takabi[6] proposed the privacy challenges and security in cloud environments. In their work they provided security of the data where the user access the cloud computing environment. Access control models are used to manage data that provide more privacy and security in the cloud computing environment. Mohammed Achemlal[8] introduced Trusted platform module enabled the security in cloud environment. Disadvantage in this paper is that it is hardware and platform based. In this paper we introduce an integrated trusted computing platform that enables security in cloud computing environment. Zhidong Shen[8] presented the security of cloud computing system enabled by trusted computing technology. In this paper they propose the system for trust computing to deliver the privacy and to provide trust platform. We proposed to

extend the trusted computing technology into a cloud environment to attain the reliable computing for the trust users requirements and to fulfill trusted cloud computing. Chi Shen[9] presented the Privacy preserving multi-keyword ranked search over encrypted cloud data. The author used the threat model where the cloud server is supposed to know only the dataset and searchable index which are outsourced from the data. We use Co-ordinate matching for the problem to overcome privacy preserving multi-keyword ranked search over encrypted data in the cloud and to establish strict privacy requirements.

3. Proposed System

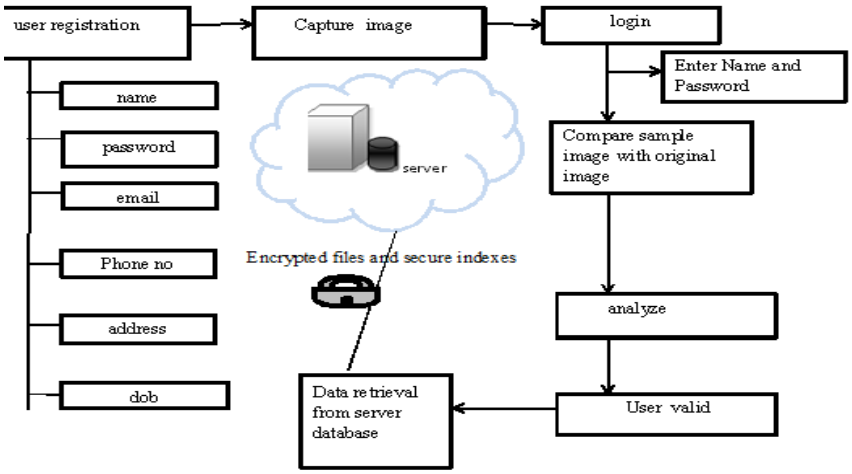


Figure 1: Architecture of the proposed model

In the existing system, robustness and trust between cloud providers and consumers is inadequate to establish the service level agreement. Investigators have predicted that the significance of trust can be managed and security can be provided based on feedbacks collected from participants. Disadvantage here is that the availability of TMS is a tough problem Owing to the unpredictable number of users and the highly dynamic nature of the cloud environment. Deceptive feedback will increase the trust result of cloud services. Multiple identities are used to distinguish the negative historical records. Identity privacy is one of the significant problem for the deployment of cloud environment. In this they used an image comparison algorithm where the user face is captured during registration time and get stored in database. With that original image we compare it with the sample image that is already stored in database. If both the image get matched then the users are identified effectively. When confidential data are subcontracted to the cloud, data holders will be worried about the security of the data in the cloud environment. Encrypting the data before sending has been considered as a important means of securing user data in contradiction of the cloud server. So in order to keep the data secure we use a symmetric key AES algorithm. Symmetric-key algorithms uses shared key concept. So only the user with private key can decrypt data. Advantage include keep the users can be identified effectively, keeps data secure, high response time. The different modules of the system are

- Registration
- Email verification
- User login
- Image capture
- Data retrieval
- Invalid user

3.1 Registration

In this module, user first have to get registered by providing the detail such as name, password, email id, dob, mobile no, address.

3.2 Email Verification

User email will be verified during the registration process. At the time of login if the user forget the password it will be sent to their respective u email id where they can get the password which it is stored permanently.

3.3 User Login

The registered user now can able to login by entering the username and password.

3.4 Image Capture

After entering name and password user face will be captured and it will compare with sample image of the user that is already stored in database. If the user is matched then the user is allowed to retrieve the data. If it does not match then it shows the result as no data match.

3.5 Data Retrieval

The data selected by the user is encrypted with the secret key. If the key match then the data is decrypted. If it does not match then there will be an error message showing that secret key does not match.

3.6 Invalid User

If an unauthorized user is trying to access with the services then the system will display an error message stating that he/she is invalid user.

3.7 Image Comparison

For every key point from both the images a descriptor is computed as below:

(i) Around every key point a pixel area of size 16 x 16 is considered.
(ii) For each sample of size 4 x 4 gradient magnitude & orientation are assigned.
(iii) A histogram of Gradient orientation showing 8 bins gives a descriptor for every 4 x 4 sample size.

(iv) For a 16 x 16 sample size around the key point a descriptor vector of dimension 4 x 4 is obtained.

(v) An approximate maximum disparity range is found by visual inspection of few matching key points in the stereo image pair.

The disparity is present in the left and right image as the stereo images are captured from different viewpoints and orientations. An area is selected around every right key point node, considering possible maximum disparity range. All the key points are found in the area selected in step 4, around a right key point node in the right image. The procedure of step (iv) and (v) is iteratively performed for all the right key points and the area around each right key point is selected considering the approximate maximum disparity range. The procedure in step (iv) and (v) is repeated for all left key points from left image performed iteratively. But here area around the left key point is a fixed sample area of size 16 x 16.

AES algorithm

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data. The data to be encrypted. This array we call the state array.

Steps involved for 128-bit block(encryption):

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

The AES decryption basically traverses the encryption algorithm in the opposite direction. The basic modules constituting AES Decryption is explain detail below:
DE crypto initially performs key-expansion on the 128-bit key block that creates all intermediate keys (which are generated from the original key during encryption for every round). The generated round key module performs the algorithm that generates a single round key. Its input is multiplexed between the user inputted key and the last round's key. The output is stored in a register to be used as input during the next iteration of the algorithm. The expansion keys module is a RAM which stores the original key and the 10 rounds of generated keys for use during the decryption algorithm.

4. Results and Discussion

Face recognition has been used in the direction of pattern recognition, neural network, fraud detection, computer vision etc. Active development of algorithms and availability of facial database are the major reasons for the fast development of face recognition. So the face comparison technology has developed as a striking solution to report many modern requirements for the confirmation of claims. So we use an image comparison algorithm where the user face is captured during registration time and get stored in database. With that original image we compare it with the sample image that is already stored in database. If both the image get matched then the users are identified effectively.

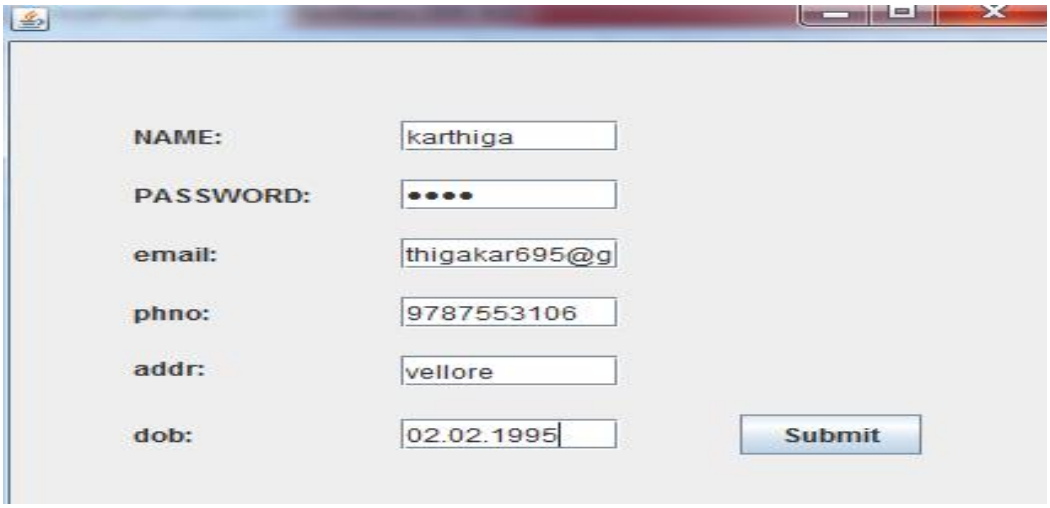


Figure 2: User Registration

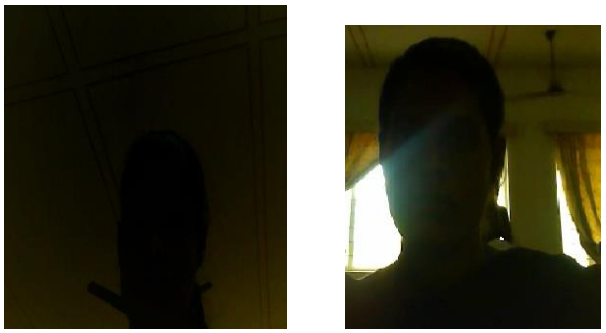


Figure 3: Comparison of original image with sample image

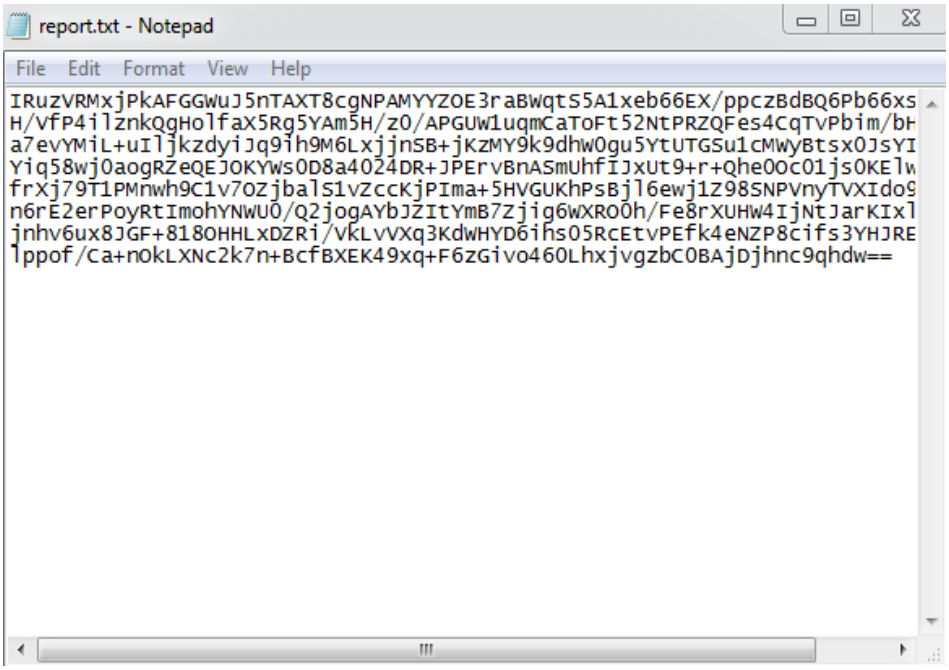


Figure 4 : Encrypted Data

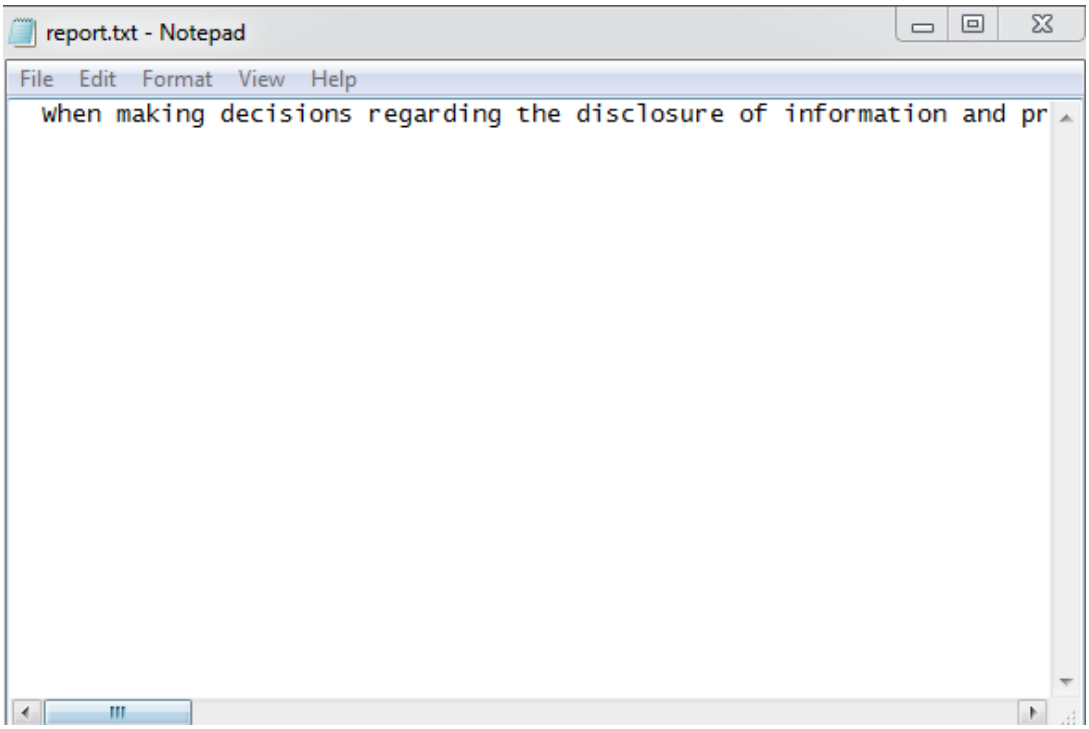
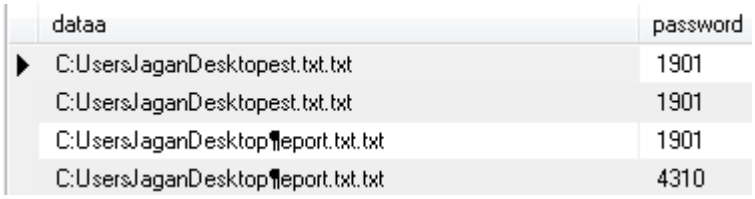


Figure 5 : Decrypting the Data



dataa	password
C:UsersJaganDesktopest.txt.txt	1901
C:UsersJaganDesktopest.txt.txt	1901
C:UsersJaganDesktop¶eport.txt.txt	1901
C:UsersJaganDesktop¶eport.txt.txt	4310

Figure 6: Data Retrieval

5. Conclusion

Establishing the trust between the cloud facilities for the users remains an important challenge in a highly distributed and dynamic cloud service. So by using image comparison algorithm and symmetric key algorithm, we identify the users against the hackers and also the data is kept secure. Hence the proposed scheme will provide security against the chosen keyword attack.

References

[1] Noor T H, Sheng Q Z, Yao L, Dustdar S and Ngu A H 2016 CloudArmor: Supporting reputation-based trust management for cloud services. *IEEE Transactions on parallel and Distributed Systems* **27(2)** 367-380.

[2] Habib S M, Ries S and Muhlhauser M 2010 Cloud computing landscape and research challenges regarding trust and reputation. *In Ubiquitous Intelligence & Computing* and 7th International Conference on Autonomic & Trusted Computing (UIC/ATC), 2010 7th International Conference on (pp. 410-415). IEEE.

[3] Guo Q, Sun D, Chang G, Sun L and Wang X 2011 Modeling and evaluation of trust in cloud computing environments. *In Advanced Computer Control (ICACC)*, 2011 3rd International Conference on (pp. 112-116). IEEE.

[4] Albeshri A and Caelli W (2010, September). Mutual protection in a cloud computing environment. *In High Performance Computing and Communications (HPCC)*, 2010 12th IEEE International Conference on (pp. 641-646). IEEE.

[5] Yan Z, Li X, Wang M and Vasilakos A 2015 Flexible data access control based on trust and reputation in cloud computing. IEEE Transactions on Cloud Computing.

[6] Habib S M, Ries S and Muhlhauser M 2011 Towards a trust management system for cloud computing. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on (pp. 933-939). IEEE.

[7] Takabi H, Joshi J B and Ahn G J 2010 Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, **8(6),** 24-31.

[8] Achemlal M, Gharout S and Gaber C 2011 Trusted platform module as an enabler for security in cloud computing. *In Network and Information Systems Security (SAR-SSI)*, 2011 Conference on (pp. 1-6). IEEE.

[9] Shen Z and Tong Q 2010 The security of cloud computing system enabled by trusted computing technology. *In Signal Processing Systems (ICSPS*), 2010 2nd International Conference on (Vol. 2, pp. V2-11). IEEE.

[10] Cao N, Wang C, Li M, Ren K and Lou W 2014 Privacy-preserving multi-keyword ranked search over encrypted cloud data. *IEEE Transactions on parallel and distributed systems*, **25(1),** 222-233.