RESEARCH ARTICLE OPEN ACCESS

Protected Intra-Conversation Information Control In An Organization

Sangeetha kalyanaraman [1], kavitha Subramani [2], s. Kunkuma sneha [3], v.maheswari [4]
Associate Professor [1],[2], U.G.Scholar [2],[3]
Department of Computer Science and Engineering, Panimalar Engineering College-Chennai

ABSTRACT
with the fast development of cloud services , huge volume of data is shared via cloud computing. Although cryptographic techniques have been utilized to provide data confidentiality in cloud , current mechanisms cannot enforce privacy issues related to multiple users in a public cloud. An Organization is an entity comprising of multiple people, such as an institution or an association ,that includes an explicit purpose and group related functions into a manageable unit to attain the objectives of the enterprise in the most significant and effective manner. Daily report enables the team manager to have an overview of how the team's project is progressing in terms of each team member's individual tasks without having to interact with one another on a daily basis. In proposed system, private cloud is used in which whatever the employee work as a task is automatically created as a PDF file in a secure way and it won't be rewritten by anyone and daily updation has been updated to the particular file using AES algorithm to encrypt the sensitive data .For accessing the PDF file by team leader , the captcha has been generated to avoid the automatically harvesting of details. If HR manager wants to percive the daily update of the team leader, then the QR code has been generated and scanned by them to get access to the file. The private cloud is secured to solve the privacy conflict problems caused by different access policies within the organization.
Keywords-Cloud services, data confidentiality, private cloud, PDF file, AES, captcha, QR code, privacy conflict.

I. INTRODUCTION

The main objective of this project is to make the work process easier in an organization. The QR code and captcha has been used to secure the resources or files from unwanted internet bots. The task which is performed by the employee is automatically converted into PDF, hence it is less time consuming. The captcha is the way to differentiate between an automated computer program and a human, it has been created to maintain a strategic distance from consequently collecting the subtleties. The main advantage of QR code is its versatility, can be used anywhere and when it is scanned, it generates a code which has to be entered by the HR manager to access the file.

Encryption is, so far, the best way you can protect the data. The most easy and handy way is to zip files and encrypt them with a password. There are some cloud services that provide local encryption and decryption of the files in addition to storage and backup. It means that the service takes care of both encrypting the files on our own computer and storing them safely on the cloud.

The Advanced Encryption Standard (AES), is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. Encryption works by taking plain text and converting it into cipher text, which is made up of seemingly random characters. Only those who have the special key can decrypt it. It was intended to be easy to implement in hardware and software, as well as in restricted environments (For eg , in a smart card) and offer good defenses against the various attack techniques. AES (Acronym of advance encryption standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES supports a block length of 128-bits and key lengths of 128,192 and 256 bits. AES comprises 3 block ciphers: AES-128,AES-192,AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-bits ,192-bits and 256-bits, respectively. The rijndael cipher was designed to accept additional block sizes and key length but for AES , those functions were not adopted.

AES uses symmetric key encryption, which involves the use of only one secret key to cipher and decipher information. AES is deemed secure because its building blocks and design principles are fully specified and it was selected as part of an opening competition.

II. LITERATURE SURVEY

[1] A Dynamic Secure Group Sharing Framework in Public Cloud Computing

Group sharing in public cloud computing, the cloud provider cannot be considered as a trusted third party because of its semi-trust nature. Thus, a protected group sharing framework for public cloud, which can effectively take

advantage of the cloud server's help but no sensitive data being exposed to attackers and cloud provider. This framework combines proxy signature , enhanced TGDH and proxy re-encryption together into a protocol. Proxy signature provide permission to one or many selected group members. The enhanced TGDH allows the group to negotiate and update the group key pairs using cloud servers. By using Proxy re-encryption, many intensive operations are delegated to cloud servers without letting any private information.

[2] Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation

The Schemes for public data integrity auditing for shared dynamic data are still not secured against the collision of cloud storage server and user revocation in cloud storage system. Here, the collusion attack is figured out and an efficient public integrity auditing scheme is provided with secure group user revocation supported with vector commitment and verifier-local revocation group signature. This Scheme supports public checking , efficient user revocation and some properties such as confidently, efficiency, countability and traceability of secure group user revocation.

[3] Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in Cloud

The cloud service providers (CSP) are not in the same trusted domain as users. To protect the data privacy against untrusted CSPs, a Revocable attribute based (RABE) encryption scheme along with identity-based encryption (IBE) and attribute-based encryption (ABE) are used to provide secure and efficient fine-grained access control and data sharing for dynamic groups. They define and enforce access policies , permit key generation to efficiently update user credentials for dynamic user group. Hence, a fine-grained access control and data sharing system for dynamic user groups in a cloud are provided.

[4] Anonymous and Traceable Group data Sharing in Cloud Computing

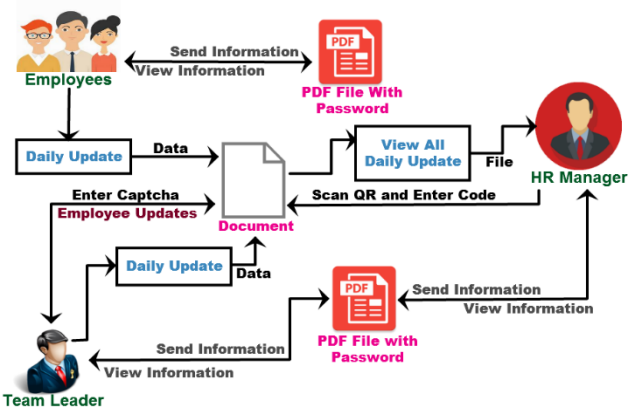
Here, data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner is enabled. The traceable group data sharing scheme is adopted to support anonymous multiple users in public clouds and group members can communicate anonymously with the help of group signature. Hence, the real identities of members can be traced easily. A common conference key is derived based on the key agreement to enable group members to share and store data securely. A symmetric balanced incomplete block design is utilized for key generation, which reduces the burden on members to derive a common conference key.

[5] Spatial Group Sparsity Regularized Nonnegative Matrix Factorization for Hyperspectral Unmixing

The group-structured prior information of hyperspectral images is incorporated into non-negative matrix factorization, where the data are arranged into spatial groups. Pixels within a local partial group share the same sparse structure in the low-rank matrix. Image segmentation is introduced for generating the spatial groups. These partial groups are represented by super pixels instead of regular shape (cross or square). The partial group structure and sparsity are integrated as a mixed-norm regularization to exploit the shared sparse pattern and to avoid loss of spatial details within the group.

III. PROPOSED SYSTEM

A modern development in time and technology requires faster information broadcasting. United ,Personalized , Intelligent Information applications are more significant in business and private lives. In proposed work, the private cloud is used in which whatever the representative undertake as a work is consequently made as a PDF record and it won't be modified by anybody, day by day refreshing has been refreshed to the specific document.



For getting to the PDF record by the team leader , the captcha has been created to generally keep away from the naturally reaping the subtleties. In the event, the HR manager needs to monitor the daily updation of the team leader, at that instance the QR code has been generated and examined by them to gain admittance to the document. The attendance has been recorded by the user login. So every time user gets login to the system the particular attendance has been taken.

IV. SYSTEM IMPLEMENTATION

The proposed work is implemented as five modules.

1. Authority Verification
2. Daily Updation
3. Captcha and QR code generation

4. Information Sharing
5. Secure PDF access

A. Authority Verification

Everytime the authentication of the team leader has to be verified by the HR manager in the organization. Whenever employee wants to login or join they have to specify the team leader identity and employee identity, then HR manager will verify the team leader details. If the team leader records are found, the employee will be accepted to authenticate.

B. Daily Updation

In any organization, the daily updating needs to be done by every employee. The report updation is typically a document prepared by employees to submit it to their team leader .A daily report updates a team leader or manager about an ongoing project. It provides an overview which describes each member's tasks and progress. The employee task on work is automatically created as a PDF file and it won't be rewritten by anyone. Hence, daily updating has been updated to the particular file.

C. Captcha and QR code Generation

Captcha is a way to differentiate between an automated computer program and a human. It has become the most widely used standard security technology, it prevents automated computer login. Captcha has been generated for the PDF file, every time the team leader want to access the file they need to enter the captcha. If the HR manager wants to see the daily update of the team leader, then the QR code has been generated and scanned by them to access the file.

D. Information Sharing

In case of any emergency issues such as any secret information , the employee's data is automatically converted into PDF and stored in the private cloud. The employee can send the secret information to the particular team leader, manager and employee within the team. The manager and team leader can also send the information to any employee within the organization.

E. Secure PDF Access

The PDF file can be accessed by anyone within the organization , but to open or read the PDF ,the password authentication will be done. The employee who gets the PDF file have to put their login credentials to access it. If someone wants to get the file who is not the particular person whom I want to sent, the PDF file could not be accessed by them because of the password authentication.

V. RESULTS

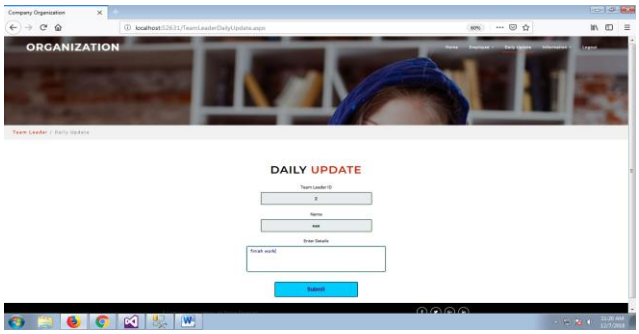


Fig 1 – Daily Update

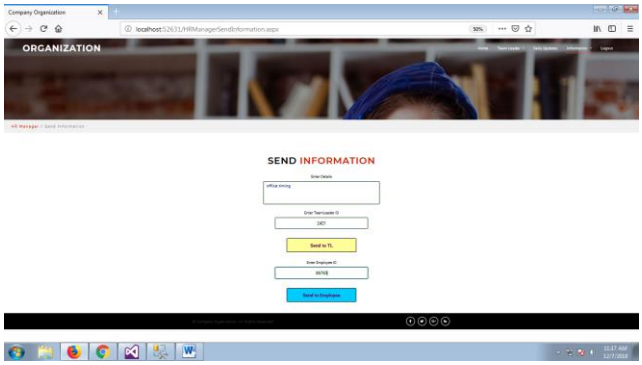


Fig2 – Send Information

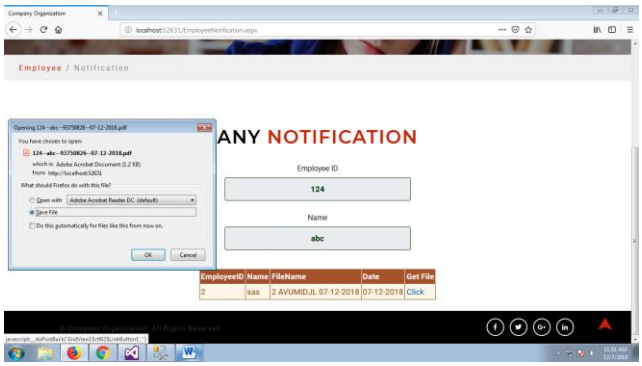


Fig 3 – Any Notification

VI. CONCLUSION

In this generation where everything needs to be faster and secured, an cutting edge improvement in time and innovation requires quicker data broadcasting joined together, customized, astute data applications are increasingly critical in business and private lives. In every organization where employee allocated with task is commenced, when task is automatically transformed into the file which is even secured access by the team leader. In

which we use captcha to prevent access from internet bots and it is even more secured accessed by the team leader. Atlast when the task is completed , the HR manager is supposed to do the inspection or verification, the QR code is generated for secure access. Thus, the private cloud is used for even more security purpose.

REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, "Cryptographic rolebased access control for secure cloud data storage systems," Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673–681.

[3] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," IEEE Systems Journal, pp. 1–10, 2015.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[5] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient rfid authentication protocol providing strong privacy and security," Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016.

[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement," Designs Codes and Cryptography, vol. 28, no. 2, pp. 119–134, 2010.

[7] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.

[8] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement (extended abstract)." Lecture Notes in Computer Science, vol. 2003, pp. 205–217, 2003.

[9] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691, 2012.

[10] B. Dan and M. Franklin, "Identity-based encryption from the weil pairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229, 2003.

[11] S. Blakewilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in IMA International Conference on Cryptography and Coding, 1997, pp. 30–45.

[12] I. Chung and Y. Bae, "The design of an efficient load balancing algorithm employing block design," Journal of Applied Mathematics and Computing, vol. 14, no. 1, pp. 343–351, 2004.

[13] O. Lee, S. Yoo, B. Park, and I. Chung, "The design and analysis of an efficient load balancing algorithm employing the symmetric balanced incomplete block design." Information Sciences, vol. 176, no. 15, pp. 2148–2160, 2006.

[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[15] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.