ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

A Novel TTP with Checksum Row Authorization Algorithm for Access Control and Data Protection in Collaborative Mobile Computing Environment

Dimple Elizabeth Baby [1], Sebastian George [2], Jessy Paul [3]

P.G Student, Dept. of Computer Science & Engineering, VJCET, Kerala, India [1]
Assistant Professor, Dept. of Computer Science & Engineering, VJCET, Kerala, India [2]
Professor, Dept. of Civil Engineering, MACE, Kothamangalam, Kerala, India [3]

Abstract: : With the introduction of smart phones with wide range of applications, the modern business world gains the advantage of all in-one gadgets with roaming work place. The collaborative computing applications found in smart phones helps in performing group work with colleagues even out of the office as all the normal computer functions are possible with the smart phones. Such applications support the interaction between people and information sharing among the participants by storing the data in common storage area. But there is high potential risk for user's security and privacy in this environment. In order to sustain privacy and security in digital collaborative environments, strong authorization and authentication framework is required and so a novel Trusted Third Party called Shielding Server is introduced which will provide strong authentication and access control mechanisms to make data sharing in collaborative computing environment more secure. Combining the finger print authentication along with conventional password authentication method will provide strong authentication. For providing good access control mechanism, the Shielding Server will classify the data into multiple levels like public, sharable and sensitive data, according to their sensitivity and impose strong access constraints for each level of data. Public data is stored as plain text and any registered user can be access it. Sharable and sensitive data are stored in an encrypted format so that only legitimate users who have the access right can decrypt the data. A novel access control mechanism based on biometric checksum block is introduced for providing privacy to the sharable data and the encryption key generated from the secret information supplied by the user will protect the sensitive data from unauthorized access.

Keywords: CRA Algorithm, Access Control, Secure Data Sharing, Privacy

I. INTRODUCTION

Mobile devices are changing the way we experience the physical world, from personal usage to work applications. The latest applications found in the smart phones helps to collaborate on projects with friends and colleagues while you are roaming around the world. Collaboration requires individuals working together in a coordinated fashion, towards a common goal. Accomplishing the goal is the primary purpose for bringing the team together. Collaborative software helps facilitate action-oriented teams working together over geographic distances by providing tools that aid communication, collaboration and the process of problem solving. Additionally, collaborative software may support project management functions, such as task assignments, time-managing deadlines, and shared calendars.

The collaborative technologies enable people to realize their ideas by sharing or taking advantage of their various resources through connected networks. Users of collaborative computing applications can store all their daily events which can be collected by their own mobile phone, for example, SMS, photos, call, movie, e-commerce information, Web service log and usage information, location information, documents, media, battery charge, personal schedule, and so on. The stored data are transferred to each user's personal database by Internet, and then they are stored and managed as a personal history with the passage of times and can be retrieved when ever required. This service allows users to share their data with other people or a certain service provider and collaborate on projects with friends, colleagues. User can install these applications on their own laptops, palmtops, mobile phone etc and store their personal data in a remote database and share the data with others as shown in figure 1.

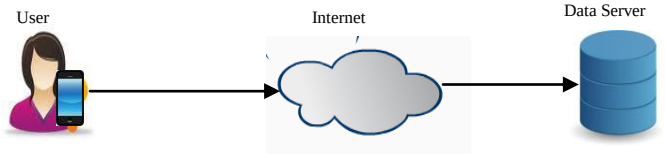

Fig. 1 User with Collaborative Computing Application

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

The storing of data in a commonly accessible structure has both a great potential for the knowledge society as well as a high risk for the user's privacy. Here in lies one of the greatest challenges for collaborative environments. That is, a continual balance must be sought between the interests of open easily accessible information with the protection of personal data and entity privacy. Strong privacy control is a major contributor to increased trust between member entities which in turn can facilitate increased participation and contribution to a collaborative environment.

In this paper a novel Trusted Third Party called Shielding Server is introduced which will provide strong authentication and resource level access control mechanisms by making use of checksum blocks.

II. BACKGROUND KNOWLEDGE

In order to sustain privacy and security in digital collaborative environments, strong authorization and authentication framework is required. Privacy is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others. Privacy in general is very subjective and means different things to different people [1] [2]. Common privacy dimensions include privacy of the person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data.

The Technical, Legal, and Community Privacy Protecting framework provides a broad information privacy solution for collaborative environments. The three key components being Technical, Legal and Community models of protection each provide three unique privacy protecting and personal data management utilities for member entity use. The integration and application of the TLC-PP framework is a significant contribution towards the delivery of a Privacy Augmented Collaborative Environment (PACE) [2] [3]. Shield Privacy provides the necessary privacy tools organizations need to build privacy protecting information systems. Shield Privacy is aimed at making information system designers and developers to consider information privacy in its own right as a design objective [3]. It forces information system owners to be aware of privacy requirements in their systems, from both a legal standpoint and as a way of building customer trust and satisfaction The guidelines like personal data minimization, separation of duty and data (SDD), information security for privacy Protection are useful in the design and implementation of collaborative environments to ensure information privacy and personal data management requirements.

Different access control mechanisms are used to provide privacy and security. Role based access control model element (RBAC) model as a whole is fundamentally defined in terms of individual users being assigned to roles and permissions being assigned to roles [6]. As such, a role is a means for naming many-to-many relationships among individual users and permissions. A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role. Permission is an approval to perform an operation on one or more RBAC protected objects

In purpose based access control mechanism, the users are required to state their access purposes along with the data access requests, and the system validates the stated access purposes by ensuring that the users are indeed allowed to access data for the particular purposes [7][8]. To facilitate the validation process, each user is granted authorizations for a set of access purposes, and an authorization for an access purpose permits users to access data with the particular purpose.

In Hippocratic database design, the purpose is the central concept around which privacy protection is build [9]. The privacy metadata tables define for each purpose and for each piece of information (attribute) collected for that purpose: the external-recipients: whom the information can be given out to, the retention-period: how long the information is stored, and the authorized-users: the set of users (applications) who can access this information.

A mediator based access control is implemented using a community authorization service (CAS) server that is responsible for managing the policies that govern access to a community's resources [10]. It also contains policy statements that specify who (which user or group) has the permission, which resource or resource group the permission is granted on, and what permission is granted. A member of a community may send the CAS server a request for a capability that will allow the user to perform a set of actions; if that request is consistent with the community's policy, the CAS server will delegate an appropriate capability back to the user. The user can then use that delegated credential to authenticate to a resource server and exercise the rights described by the capability.

III. SHIELDING SERVER WITH STRONG AUTHENTICATION AND CHECKSUM BLOCK BASED ACCESS CONTROL

Collaborative computing applications found in smart phones are designed for note taking and archiving and helps to remember things you like in your everyday life. Since memory of smart phone is very small, these kinds of applications help the user to store a large amount of data in a remote personal storage server with the help of internet and retrieve the data whenever needs. Users will feel that their personal storage memories are on every computer, phone and device they use. The user can collaborate on projects with friends and colleagues. But data stored in the storage server is not secure as no encryption is used and no special access control mechanisms used for providing privacy.

The proposed scheme introduces a novel Trusted Third Party called Shielding Server, for providing security using strong encryption methods and privacy through multilevel data classification and access control. Shielding server

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

situated between user and storage server, will shield the data storage server from direct access of users. Only the legitimate user who has access right can contact the storage server. In order to provide security, strong authentication method like finger print verification is included, along with traditional method like password authentication. For providing privacy data is classified into different levels like public, sharable and sensitive according to its sensitivity (Table I) and separate encryption keys are used for each level of data. User has to prove that he has the permission to access a particular data at the time of retrieval. If the user is valid one, then decryption key for the requested data will be obtained.

A. Notations Used

This section introduces some notations used throughout this paper and their meaning

- E/D : Encryption/Decryption Algorithm
- fin : finger print image
- k_pwd : key generated from password
- f1 : encrypted finger print image
- f_Cuij : j^{th} sensitive level file of user i
- k_Cuij : sensitive level data encryption key
- e1/e2 : encrypted content
- f_BUij : j^{th} sharable file of user i
- k_rand : random key generated at mobile device for encryption of file before sending to shielding server
- k_BUij : original sharable level key generated by original shielding server for user i's j^{th} sharable level file
- f_AUij : j^{th} public file of user i
- xcks_un : XORed checksum of file and finger print image of user n
- XCKS_BLOCK fi : n blocks of XORed checksum of file fi and finger print image of n users
- MDi : mobile device
- PWD' : password
- B / B' : finger print image

B. Entities Involved in Proposed Scheme

The proposed scheme has three main parties: a user/a mobile device, a Shielding server, and a data server (S).The Shielding Server is located in front of storage server as shown in figure 2. It authenticates a legitimate user and verifies the accessible authorization to data which the user wants to retrieve. In order to achieve this, Shielding server manages all of the things related to authentication such as enrolment of biometric information, personal information, and generation of instances for authentication processes, with powerful computational and storage abilities. All the data of each user are stored in the user's personal DB, which is managed by a server manager S. The Shielding Server knows secret keys of sharable data so that it can decrypt the data stored in personal DBs. The secret keys should not be given to any administrator and it means that the server cannot decrypt any data. A data server S only has to store all data and implement queries of Shielding Server.

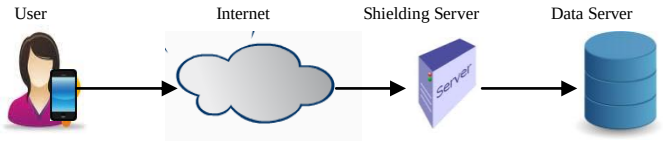

Fig. 2 Shielding Server (TTP) situated between user and data server.

C. *Classification of Information according to sensitivity*

All of the data to be stored in storage server are classified into three categories according to their sensitivity. This classifying standard is determined by a user with his or her subjective standard. Users can determine the level of data when they store with pop-up message. It is associated with self regulation of privacy. In this way, users can control their own information by themselves.

Public data is the information that anyone can access and share the information.

Sharable data is not public but sharable information so that this level of information requires to be encrypted with distinctive encryption keys for each file. For providing security while transferring data, encryptions are implemented in each user's mobile phone and then the encrypted data are transferred to Shielding Server. In order to share this level of information, the original keys need to be managed by Shielding Server because valid users' access authorization can be changed dynamically.

Sensitive level information is highly sensitive information and the owner does not share this information with anyone.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

TABLE I
CLASSIFICATION OF INFORMATION LEVEL

Information Level	Storage format in server	Properties
Public	Plaintext	This level is not so sensitive and can be disclosed in public
Sharable	Cipher Text	Sensitive but sharable. This should be encrypted and decrypted only by authorized users
Sensitive	Cipher Text	Highly sensitive information. It should be decrypted only by owner

D. Finger Print Authentication

Fingerprint authentication is one of many biometric forms of human identification. A fingerprint sensor captures a digital image of a fingerprint pattern of the user at the time of registration. The captured image will be encrypted using key generated from the password of the user and stored at the Shielding Server.

$$f1 = E_{k\_pwd}(fin)$$

At the time of login of the user, this encrypted image will be shipped back to the user and decrypted correctly if user could submit correct password. This image will be compared with the newly submitted image for checking whether the user is valid or not.

$$fin = D_{k\_pwd}(f1)$$

E. Sensitive level data key generation

The sensitive data should be encrypted and stored in a secure manner. Sensitive level data can be decrypted only by the owner and so key used for encryption and decryption should be strong enough. A strong key can be generated from a secret information provided by the user at the time of file saving. The secret information is just like a password and it has to be remembered by the user for decrypting the file. The decryption of the file is possible only if the user supplies same secret information used at the time of file saving. The advantage of this method is that sensitive data key is not stored anywhere and only the owner can decrypt the file.

F. Encryption and Decryption of the file

The sharable level and sensitive level file is encrypted using separate key.

[Encryption]

1) Sensitive level file

First Encryption: Encryption at the mobile device
$e1 = E_{k\_Cuij}(f\_CUij)$

2) Sharable level file

First Encryption: Encryption at the mobile device
$e1 = E_{k\_rand}(f\_BUij)$

Second Encryption: Encryption at Shielding Server by original key
$e2 = E_{k\_BUij}(e1)$

3) Public level file

First Encryption: Encryption at the mobile device
$e1 = E_{k\_rand}(f\_AUij)$

[Decryption]

Sensitive level file

First Decryption: Decryption at the mobile device
$D_{k\_Cuij}(e1) = f\_CUij$

1) Sharable level file

First Decryption: At Shielding Server by original key, if the user has the permission to access the file.
$D_{k\_BUij}(e2) = e1$

Second Decryption: At mobile device, using a random key used for secure transfer of file
$D_{k\_rand}(e1) = f\_BUij$

2) Public level file

First Decryption: Decryption at the mobile device
$D_{k\_rand}(e1) = f\_AUij$

G. *Checksum Row Based Access Control Mechanism*

Corresponding to each sharable file stored at Data Server, a checksum row will be formed (Fig.4). This checksum block will corresponds to the list of users who have the permission to access the file. User list will include the set of users who are selected by the owner of the file to whom he is willing to share the file. Corresponding to each sharable file, Shielding server will create a checksum row of n blocks if n users are selected by the owner of the file.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

$XCKS\_BLOCK_{fi} = xcks\_u1 + xcks\_u2 + xcks\_u3 \ldots xcks\_un$,
where xcks_un is formed by XOR-ing checksum of file fi and checksum of finger print image of user n.

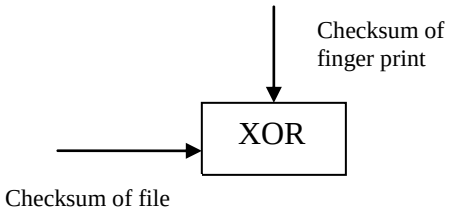

Fig. 3 one block corresponding to a single user

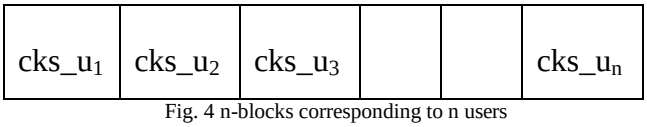

Fig. 4 n-blocks corresponding to n users

The authorization to a particular file is stored as the checksum blocks. No one can understand who all have the permission to a particular file by examining the checksum block. When a user request for a particular file, the Shielding server will XOR the checksum of finger print image and file content and search in whole n-blocks to find a match. If the requested user has the permission to access the file, then a matching block will be obtained.

H. Checksum Row Authorization (CRA) Algorithm

Algorithm 1 is a pseudo code for CRA algorithm. FILE_SET is the set of all files and IMG_SET is the set of all finger print images of users to whom a particular file is to be shared. If the user is willing to share f number of files with others, the algorithm will produce f rows of checksum block (CKS_ROWf). The variable FLCKS holds the checksum of file and BLOCKui is the XORed checksum of finger print image and the file.

Algorithm 1. Checksum Row Authorization (CRA)
Input: Set of files: FILE_SET, Set of images IMG_SET
Output: f number of checksum row

```
1:  begin
2:      for each file f Є FILE_SET do
3:          find checksum of f and assign it to FLCKS
4:          for each image i Є IMG_SET do
5:              find checksum of I and assign it to iCKS
6:              XOR FLCKS and iCKS and assign it to BLOCKui
7:              append BLOCKui to the end of CKS_ROWf
8:          end
9:          save CKS_ROWf and set CKS_ROWf to null
10:     end
11: end
```

I. Whole Protocol Used

For establishing a secure communication path between user and Shielding Server, public-private key pair is used. The public key of Shielding Server is distributed to the users. A public–private key pair will be created for each login session of the user and request and public key of the user will be sent to Shielding Server after encrypting them with public key of Shielding Server. The following steps explain the whole protocol.

[User]

1. User i inputs his password pwd' and fingerprint B' on each sensor of the mobile device.
2. Encrypted finger print stored (B) at Shielding Server will be shipped to MDi and decrypt it with key generated from the password. Compare B and B'
3. If B= = B', the user is valid one and user has the right to upload or download file. A public-private key pair is used for establishing a secured communication path and public key must be sent to Shielding Server after encrypting with its public key.

4. If upload mode is chosen by user, select the file to be stored and its level of access send it to Shielding server. If public data, it is stored as plain text. If sharable data list of users who have the access permission to the file must be sent. If sensitive level data, it is encrypted using sensitive level key obtained from the secret

information supplied by the user and sent to Shielding Server. All communications to Shielding Server will be encrypted using its public key.

5. If download mode is selected, user has to prove that the user has the permission to the requested file.

   [Shielding Server]

6. If the mode of operation is uploading and access level is either public or sensitive, Shielding Server will send the file to Data Server by encrypting it using a symmetric key shared between Shielding Server and Data Server. If sharable level is chosen, checksum block for authorization will be formed from user list and stored at Shielding Server. Then encrypt data by sharable level key randomly generated and reencrypt it using symmetric key shared between Shielding Server and Data Server for secure data transfer. The original sharable data key is stored at Shielding Server

7. If mode of operation is downloading, Shielding Server will first check whether the user has the access right to the requested file. If the user is authorized one the request is forwarded to Data Server

   [Data Server]

8. Data Server will decrypt the request from Shielding Server by the symmetric key shared between Shielding Server and Data Server.

9. If the request is to upload the file, Data Server will store the file. If the request is to download the file, Data Server will retrieve the content sent to Shielding Server by encrypting it using same symmetric key.

   [Shielding Server]

10. If level public or sensitive file is requested by the user Shielding Server simply decrypt the result obtained from Data server and sent to user after encrypting it with a newly generated random key. This key will be sent to user after encrypting it using user's public key.

11. If the requested file is sharable, first the result from data server is decrypted using symmetric key. Then decrypt the content by the original key stored at the Shielding Server and sent to user after encrypting it with a newly generated random key. This key will be sent to user after encrypting it using user's public key.

    [User]

12. If public level or sharable level file is requested, the result is simply decrypted for obtaining the actual content.

13. If sensitive level file is requested, the result is decrypted using sensitive level key obtained from the secret information.

IV. IMPLEMENTATION

The following section describes different module and the implementation details.

A. Registration and Login

User must register with Shielding Server by submitting user id, password and biometric information (finger print).Here fingerprint authentication is added along with the traditional method of user id and password for getting strong authentication. After registration, Shielding Server has to finger print (B) after encrypting it using key generated from password.

Key of 128-bit length can obtained after applying MD5 to the user's password and by using AES encryption byte array of finger print image can be stored

RSA algorithm is used for secure communication channel establishment between user and Shielding Server. Shielding server's public key is distributed to all users and a public-private key pair will be generated for each login session of the user.

B. Data Storage

By using collaborative computing applications in smart phones, user can store SMS, Contacts, and files in a remote personal database. The user will classify the data at time of storage. Different levels of data include public, sharable and sensitive and different encryption keys are used accordingly. Data encryption is performed by AES algorithm.

Each time when a sharable file is stored at Data Server, the user must select multiple persons from the group that the user is willing to share file. In other words, along with the file stored, user must selects name of persons from list who

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

can access the user's file and it has to send to Shielding Server. The key for sharable data is generated by the Shielding Server and it will hold a file details table with the following structure.

TABLE III
FILE DETAILS TABLE

File id	File name	Owner	File type	Key

The field file id corresponds to the unique file id, file name corresponds the name of the file storing. File type shows the level of storage and key is the encryption key for the file. Rows created for the file details table during the execution is shown below in table III. The filed file type can have values zero, one and two. The value zero corresponds to the public level, one corresponds to the sharable level and two corresponds to the sensitive level data.

TABLE III
THE SAMPLE DATA FOR THE FILE DETAILS TABLE

fileid	filename	owner	filetype	keyv
63	abs.doc	linu	1	3mTUmHuaP0LbBFOpKn6fVhnogO7zB0dKPx0NzptYiOKZRrY6Hy8r0dNEFOa8QVF
64	Front pagesnew (1).doc	linu	1	cbpVMlMohZeRaNohxfG5V6lFxs3Ncv4sJcnZlaHbGhR01IY5gOcpjyYIC
65	zzz.doc	linu	1	5L6q1INjXRYRVI9YjKZ50g2t6mu9iQzY8sEy5hBM802BmQcq3HTYVhfiLpTkrigyliYOjQxd8DV1ehLJ9thbQL7vJEtB
66	test.doc	linu	1	3CQEjrg2T1yyRFxFACAyCaRbS5XCCFJS87p3XKZnf5UFlNHkvZ5gskT6S22kGp6s2A56qMLATNA3zLOdevQk40
67	test.doc	linu	2	VSjLOPF4ACkeuhJ8TxjHDSc6KAbA2F6oCBHa90X54JbUTlLbVTNxj
68	abs.doc	linu	1	a8MvADZgbyibqHsRJzYOQ2ORPArncIdmX3Ql9NXE7KNuQQrhbNLGldpcifYZFKt2gdR4JFa2dNIEVeT9QIbds7i
69	abs.doc	linu	1	8HCn5lXtRpv21NqLQrbBjKtUZihaEcCtzIxg8FitnytNIv8eACYBUL9qXtdICMIAd7UTE42hfIpVZFOyoyS85m
70	abs.doc	linu	2	csKdiyqUIHKOvT8Rvtuqge38k3XU64xePTjMKuarLNQpEQ1FStHSKjJUc3Tnq9hlhDZ1ZpRsVt3DdRUAiROVuh4I16j4nJkRGg7

C. Checksum Row Authorization

Checksum of the file is obtained after applying MD5 algorithm to the file content. Similarly, each user's finger print byte stream is taken and applying MD5 algorithm. After that, XOR the two checksum results. For the implementation of checksum row authorization, we can use the permission table with the following structure. The field file id corresponds to the unique file id and userid indicates to the share corresponds to the authorized users to whom the file is shared. The authorized user list is sent to the Shielding Server by the user. The checksum row created in the permission table during the execution is shown below in table V

TABLE IIIV
PERMISSION TABLE

File id	User id

TABLE V
THE SAMPLE DATA FOR THE PERMISSION TABLE

fileid	userid
69	19 7 25 -46 -115 -36 -128 104 -101 119 104 -23 78 81 35 -17< 125 96 -117 -1 -64 -41 14 112 100 -83 20 0 -5 -46 64 -52<
68	-29 -100 43 -105 92 97 -70 -84 -123 -119 104 -54 -44 -86 70 -117< -79 -91 64 97 8 -124 111 -58 -27 79 32 125 83 113 73 52<
66	-45 122 -127 37 83 -99 -125 1 7 -66 27 96 -21 -5 -41 -111< -19 -93 -9 39 -13 93 101 17 29 14 24 15 43 -112 -84 80< -47 -3 14 -4 -22 -77 62 99 -126 18 44 81 25 -56 -64 -52< 54 -30 -59 -98 7 -49 38 -26 39 104 29 62 24 32 119 72<
63	-77 -119 -123 -117 122 48 118 127 70 52 32 -116 -49 -11 47 -5< 84 -106 78 -23 -105 76 110 -6 -29 78 17 -29 -50 29 -104 127<
65	25 -41 44 1 92 -18 -78 44 -1 -88 -121 25 -35 -64 122 -20< 119 -80 -66 44 17 -27 60 52 0 114 -5 -16 104 67 25 -49< 0 32 34 100 96 -124 94 -96 73 33 28 107 -128 54 10 44< 73 105 -56 46 -79 37 -38 36 26 -62 -8 -97 -88 40 98 14<

IV. CONCLUSION

Collaborative computing has emerged as a new way for interaction between people and it will support information sharing among the participants. The collaborative computing applications in smart phones promote teamwork by allowing users to share their data with the members of the team. In order to provide information privacy and security in this environment, a Trusted Third Party called Shielding Server is introduced. Shielding server will shield the data storage server from direct access of users. Only the legitimate user who has access right can contact the storage server. Strong authentication mechanism like finger print identification is included so that only valid user can access the storage server. For providing information security, the data is stored in an encrypted format and for privacy, data is classified into multiple levels according to their sensitivity and strong authorization methods are introduced for each level of data. A secure communication path is established using public-private key pairs for request-replay transfer. The proposed system will covers functions like private key management of PKI, biometric management, data sharing over an encrypted database, etc. This scheme is secure against all the attacks from various routes and provides privacy preserving access control and therefore, can be applied to other applications which require strong authentication and access control mechanisms.

REFERENCES

[1] L. Kagal, T. Finin, A. Joshi, and S. Greenspan, "Security and Privacy Challenges in Open and Dynamic Environments," IEEE Trans. Computers, vol. 39, no. 6, pp. 89-91, June 2006.
[2] G. Skinner, "The TLC-PP Framework for Delivering a Privacy Augmented Collaborative Environment (PACE)," Proc. Third Int'l Conf. Collaborative Computing, Networking, Applications and Worksharing, 2007.
[3] G. Skinner, "Shield Privacy: A Conceptual Framework for Information Privacy and Data Access Controls," WSEAS Trans. Computers, vol. 5, no. 6, pp. 1375-1384, 2006
[4] D. Argarwal, M. Thompson, M. Perry, and M. Lorch, "A New Security Model for Collaborative Environments," Paper LBNL- 52894, Lawrence Berkeley Nat'l Laboratory, Univ. of California, 2003.
[5] A.P. McAfee, "Enterprise 2.0: The Dawn of Emergent Collaboration," MIT Sloan Management Rev., vol. 47, no. 3, pp. 21-28, 2006.
[6] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila "Proposed NIST Standard for Role-Based Access Control", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001
[7] J. Byun, E. Bertino, and N. Li, "Purpose Based Access Control of Complex Data for Privacy Protection," Proc. 10th ACM Symp. Access Control Models and Technologies, pp. 102-110, 2005.
[8] J. Byun, E. Bertino, and N. Li, "Purpose-Based Access Control for Privacy Protection in Relational Database Systems," Technical Report 2004-52, Purdue Univ., 2004.
[9] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic Databases," Proc. 28th Int'l Conf. Very Large Databases (VLDB), 2002.
[10] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, "A Community Authorization Service for Group Collaboration," Proc. Third Int'l Workshop Policies for Distributed Systems and Networks, pp. 50-59, 2002.
[11] A.A. Ross, K. Nandakumar, and A.K. Jain, Handbook of Multibiometrics, first ed. Springer, 2006.
[12] B. Gelbord and G. Roelofsen, "A Solution to Privacy Issues in the Use of Biometrics in PKI," Proc. WAP2001, 2001.

BIOGRAPHY

Dimple Elizabeth Baby received the B.Tech degree in Information Technology from Viswajyothi College of Engineering and Technology, Vazhakulam, Mahatma Gandhi University, in 2010. She is currently doing her MTech in Computer Science and Engineering at Viswajyothi College of Engineering and Technology, Vazhakulam.

Sebastian George has been serving as Assistant Professor in CSE department at Viswajyothi College of Engineering and Technology, Vazhakulam. He received the B.Tech degree in Computer Science and Engineering from St.Joseph's College of Engineering and Technology, Palai and completed Post Graduation from Middlesex University (England).

Jessy Paul is Professor in Civil Department at M.A College of Engineering, Kothamangalam. She received the B.Tech degree in Civil Engineering from M.A College of Engineering, Kothamangalam and received M.Tech from IIT, Mumbai.