ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

Safeguarding Email Content in the Cloud through Conditional Identity-Based Broadcast Proxy Re-Encryption

Ms.Maheshwari[1], K.Shravani varma[2], K.Sangeetha[3], G.Jhansi[4]

ABSTRACT

Recently, a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), identity-based PRE (IPRE) and broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a versatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key are independent of the original receivers of any initial ciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure email systems based on Pretty Good Privacy protocol or identity-based encryption.

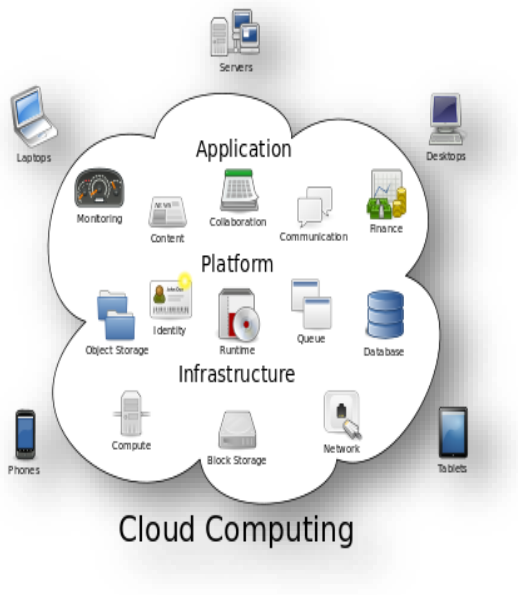
I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of

[1]Assitant Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, munnellimaheshwari@gmail.com
[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, India.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Characteristics and Services Models:

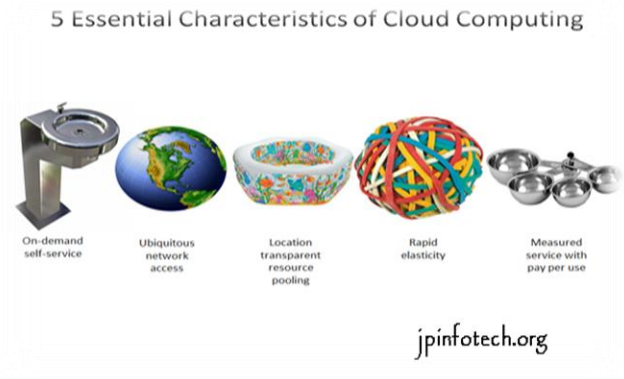
The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

client platforms (e.g., mobile phones, laptops, and PDAs).

- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.



Characteristics of cloud computing

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.
7. **Traffic:** Deals with spike in traffic with quick deployment of additional instances to handle the load.

II. LITERATURE REVIEW

Identity-Based Proxy Re-Encryption Scheme Using Fog Computing and Anonymous Key Generation , Han-Yu Lin,Tung-Tso Tsai, Yan-Rong Fan, In the fog computing architecture, a fog is a node closer to clients and responsible for responding to users' requests as well as forwarding messages to clouds. In some medical applications such as the remote healthcare, a sensor of patients will first send encrypted data of sensed information to a nearby fog such that the fog acting as a re-encryption proxy could generate a re-encrypted ciphertext designated for requested data users in the cloud. Specifically, a data user can request access to cloud ciphertexts by sending a query to the fog node that will forward this query to the corresponding data owner who preserves the right to grant or deny the permission to access his/her data. When the access request is granted, the fog node will obtain a unique re-encryption key for carrying out the re-encryption process. Although some previous concepts have been proposed to fulfill these application requirements, they either have known security flaws or incur higher computational complexity. In this work, we present an identity-based proxy re-encryption scheme on the basis of the fog computing architecture. Our identity-based mechanism uses public channels for key distribution and avoids the troublesome problem of key escrow. We also formally prove that the proposed protocol is secure in the IND-PrID-CPA notion. Furthermore, we show that our work exhibits better performance in terms of computational complexity.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

III. EXISTING SYSTEM:

- Effective health information exchange needs to be standardized for interoperable health information exchange between hospitals. Especially, clinical document standardization lies at the core of guaranteeing interoperability.
- It takes increasing amount of time for the medical personnel as the amount of exchanged CDA document increases because more documents means that data are distributed in different documents. This significantly delays the medical personnel in making decisions. Hence, when all of the CDA documents are integrated into a single document, the medical personnel is empowered to review the patient's clinical history conveniently in chronological order per clinical section and the follow-up care service can be delivered more effectively. Unfortunately for now, a solution that integrates multiple CDA documents into one does not exist yet to the best of our knowledge and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology.

Disadvantages of existing system:

1. The HIS development platforms for hospitals vary so greatly that generation of CDA documents in each hospital invariably requires a separate CDA generation system. Also, hospitals are very reluctant to adopt a new system unless it is absolutely necessary for provision of care. As a result, the adoption rate of EHR is very low except for in a few handful countries.
2. Unfortunately for now, a solution that integrates multiple CDA documents into one does not exist yet to the best of our knowledge and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology.
3. To establish confidence in HIE interoperability, more HIS's need to support CDA. However, the structure of CDA is very complex and the production of correct CDA document is hard to achieve without deep understanding of the CDA standard and sufficient experience with it.

4. PROPOSED SYSTEM:

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

1. In this paper we present (1) a CDA document generation system that generates CDA documents on different developing platforms and (2) a CDA document integration system that integrates multiple CDA documents scattered in different hospitals for each patient.

2. CDA Generation API generates CDA documents on cloud.

3. CDA Generation Interface uses the API provided by the cloud and relays the input data and receives

4. CDA documents generated in the cloud.

5. Template Manager is responsible for managing the CDA documents generated in the cloud server. Our system uses CCD document templates.

6. CDA Generator collects patient data from hospitals and generates CDA documents in the template formats as suggested by the Template Manager.

7. CDA Validator inspects whether the generated CDA document complies with the CDA schema standard.

Advantages of proposed system:

1.Hospital systems can simply extend their existing system rather than completely replacing it with a new system. Second, it becomes unnecessary for hospitals to train their personnel to generate, integrate, and view standard-compliant CDA documents.

2. The cloud CDA generation service produces documents in the CDA format approved by the National Institute of Standards and Technology (NIST).

3. If this service is provided for free at low price to hospitals, existing EHR are more likely to consider adoption of CDA in their practices.

4. Interoperability between hospitals not only helps improve patient safety and quality of care but also reduce time and resources spent on data format conversion.

IV. MODULE

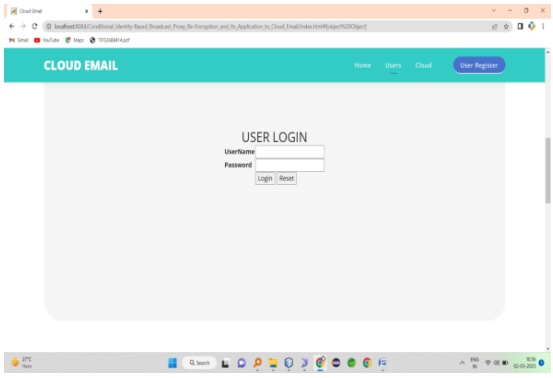
1. USER(SENDER)
2. USER(RECEIVER)
3. CLOUD

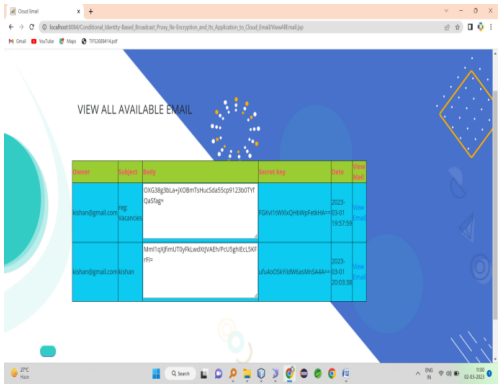
V. MODULE DECRYPTION

1. **USER (SENDER):**

   Here user (sender) should register with application then the user should login with the application after successful login he can perform some operations such as add cloud details, encrypt email and upload to cloud, view history, view request and send re encryption request to cloud then logout.

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024



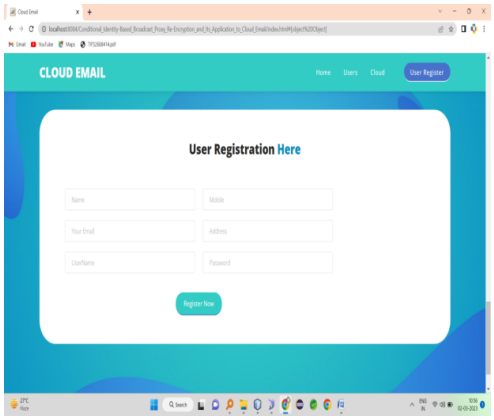


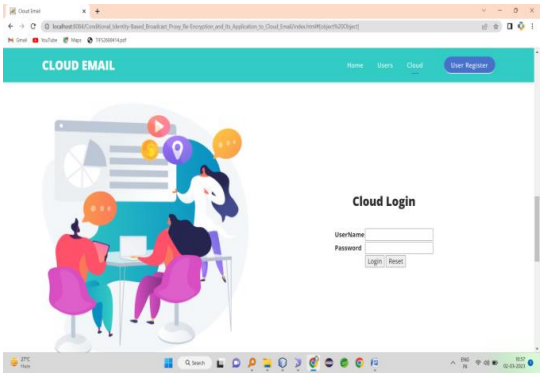
2. USER(RECEIVER)

Here user (receiver) should register with application then the user should login with the application after successful login he can perform some operations such as view all emails and send request for email owner to view the email, view status and verify decrypt key if the verification is successful then can read email and have the chance to download email and logout.

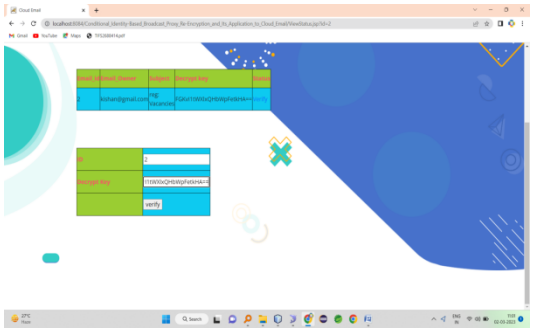
3. CLOUD

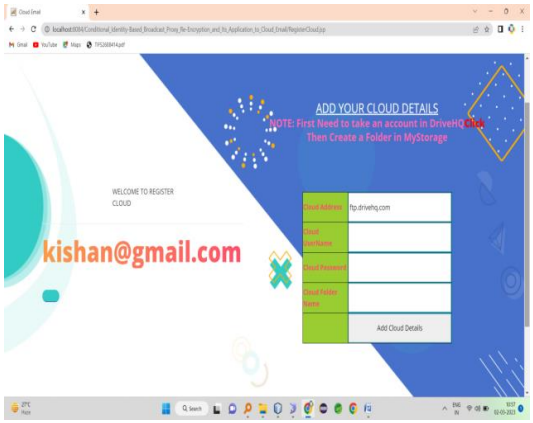
Here cloud is the module should directly login with the application after successful login he can perform some operations such as view all users and view all emails and view re-encryption request and perform re-encryption and send the re-encrypt email with decrypt key to the receiver and logout.





INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST
ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024





VI. CONCLUSION

This paper presented a new kind of PRE concept called conditional identity-based broadcast proxy re-encryption (CIBPRE), as well as its IND-sID-CPA security definitions. The CIBPRE is a general concept equipped with the capabilities of conditional PRE, Identity-based PRE and broadcast PRE. The IND-sID-CPA security definition of CIBPRE incorported the security requirements of CPRE, IPRE and BPRE.

CIBPRE inherits the advantages of CPRE, IPRE and BPRE for applications. It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE users takes their identities as public keys to encrypt data. It avoids a user to fetch and verify other users' certificates before encrypting his data. Moreover, it allows a user to generate a broadcast ciphertext for multiple receivers and share his outsourced encrypted data to multiple
receivers in a batch manner.

we instantiated the first CIBPRE scheme based on the Identity-based broadcast encryption in [30]. Upon the provable security of the IBBE scheme and the DBDH
assumption, the instance of CIBPRE is provably IND-Sidcpa secure in the RO model. It indicates that without the corresponding private key or the right to share a user's outsourced data, one can learn nothing about the user's data.

Finally, we compared the proposed CIBPRE scheme with similar works and the comparison confirms the advantages of our CIBPRE scheme. We built the encrypted cloud email system based our CIBPRE scheme. Compared with the previous techniques such as PGP and IBE, our CIBPRE-based system is much more efficient in the

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

aspect of communication and more practical in user experience.

VII. REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Crytographic Techn.: Adv. Cryptol., 1998, pp. 127–144.

[2] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi, "A closer look at PKI: Security and efficiency," in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, 2007, pp. 458–475.

[3] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288–306.

[4] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 247–267.

[5] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Proc. 10th Int. Conf. Inf. Security, 2007, pp. 189–202.

[6] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identity- based proxy re-encryption scheme and its application in healthcare," in Proc. 5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.

[7] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., 2011, pp. 1–5.

[8] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles," in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–146.

[9] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional proxy broadcast re-encryption," in Proc. 14th Australasian Conf. Inf. Security Privacy, 2009, pp. 327–342.

[10] Q. Tang, "Type-based proxy re-encryption and its construction," in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol., 2008, pp. 130–144.

[11] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in Proc. 4th Int. Symp. Inf., Comput. Commun.Security, 2009,

pp. 322–332. 78 IEEE TRANSACTIONS ON COMPUTERS, VOL. 65, NO. 1, JANUARY 2016

[12] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

proxy re-encryption with chosen-ciphertext security," in Proc. 12th Int. Conf. Inf. Security, 2009, pp. 151–166.

[13] L. Fang, W. Susilo, and J. Wang, "Anonymous conditional proxy re-encryption without random oracle," in Proc. 3rd Int. Conf. Provable Security, 2009, pp. 47–60.

[14] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, "A conditional proxy broadcast re-encryption scheme supporting timedrelease," in Proc. 9th Int. Conf. Inf. Security Practice Experience, 2013, pp. 132–146.

[15] P. R. Zimmermann, PGP Source Code and Internals. Cambridge, MA, USA: MIT Press, 1995.

[16] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol.: Adv. Cryptol., 2001, pp. 213–239.

[17] Radicati Group. (2014). Cloud business email market, 2014-2018 [Online]. Available: http://www.radicati.com/wp/wp-content/uploads/2014/10/Cloud-Business-Email-Market-2014-2018-Executiv Summary.pdf

[18] Proofpoint Group. (2012). Cloud-based archiving vs. on-premises legacy archiving [Online]. Available: http://video.proofpoint.com/id/cloud-based-archiving-vs.-on-premises-legacy-archiving-TCO-white-paper

[19] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Security, vol. 9, pp. 1–30, 2006.

[20] R. H. Deng, J. Weng, S. Liu, and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings," Cryptol. Netw. Security, vol. 5339, pp. 1–17, 2008.

[21] V. Kirtane and C. P. Rangan, "RSA-TBOS signcryption with proxy re-encryption," in Proc. 8th ACM Workshop Digital Rights Manage., 2008, pp. 59–66.

[22] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in Proc. 11th Int. Workshop Practice Theory, 2008, pp. 360–379.

[23] J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in Proc. 12th Int. Conf. Practice Theory Public Key Cryptography, 2009, pp. 357–176.

ISSN 2229-6107
www.ijpast.in
Vol 14 Issuse 1 Jan 2024

[24] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., 2009, pp. 279–294.

[25] J. Shao, P. Liu, G. Wei, and Y. Ling, "Anonymous proxy reencryption," Security Commun. Netw., vol. 5, no. 5, 2012, pp. 439–449.

[26] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy reencryption," in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 185–194.

[27] T. Matsuda, R. Nishimaki, and K. Tanaka, "CCA proxy re-encryption without bilinear maps in the standard model," in Proc. 13th Int. Conf. Practice Theory Public Key Cryptography, 2010, pp. 261–278.

[28] K. Liang, M. H. Au, J. K. Liu, X. Qi, W. Susilo, X. P. Tran, D. S. Wong, and G. Yang, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[29] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, " An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. Eur. Symp. Res. Comput. Security, 2014, pp. 257–272.

[30] C. Delerabl_ee, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in Proc. 13th Int. Conf. Theory Appl. Cryptol. Inf. Security: Adv. Cryptol., 2007, pp. 200–215.

[31] D. Boneh and X. Boyen, "Efficient selective-id secure identitybased encryption without random oracles," in Proc. Adv. Cryptol., 2004, pp. 223–238.

[32] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in Proc. 24th Annu. Int. Cryptol. Conf.: Adv. Cryptol., 2004, pp. 197–206.