ISSN 22773061

Secure Data Forwarding in Cloud Storage System by using UMIB Proxy re-encryption

P Radha Krishna Reddy[1], S Sivaramaiah[2], U Sesadri[3]
M Tech (CSE) [1]
Asst Prof CSE[2]
HOD CSE[3]
VITS, under JNTUA
Pallavali@gmail.com[1]

Abstract:

The cloud storage system is a model consists of networked online collection of storage servers that provides long-term storage services over the Internet hosted by the third parties. Storing data in third party's cloud system creates serious problems over data confidentiality & authorization. The normal encryption schemes may protect data confidentiality from unauthorized users, but these techniques are limited based on their functionality because only few operations are supported over encrypted data.It's a challenging task to construct secure storage system with multiple functionalities, if the storage system is distributed. In this paper we developed a secure distributed storage system by using (UMIB-PRE) Unidirectional and Multiuse Identity based proxy re encryption technique with decentralized erasure code. The main theme of this UMIB proxy re encryption is to support encoding, storing and forwarding operations over encrypted data. Our method full supports encryption, decryption, encoding and forwarding techniques. We also suggest possible parameters for these key servers and storage servers as well. These parameters will give robustness to storage servers.

Key Words: Proxy Re Encryption, Cloud Storage System, Unidirectional and Multiuse, Identity Based PRE.

ISSN 22773061

1. Introduction

1.1 Overview

Cloud computing provides the demanding need to store information securely, operations, contribution and analyze immense amounts of knotty data to illustrate patterns and drifts in order to improve the quality. Cloud computing is the dream of computing as a service, where the customers of cloud stores data, utilization of high quality networks, servers and application services. The following are the few advantages of cloud computing: ubiquitous network access, independent resource location pooling, on demand self-service, rapid source elasticity, usage based costing, risk transferences etc. [11] Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. We are conducting research on secure cloud computing. (PRKR, 2012) Due to the extensive complexity of the cloud, we contend that it will be difficult to provide a holistic solution to securing the cloud, at present. The main goal is to enhance the cloud computing with secure storage. Our preparation is secure clouds that consist of secure hardware, software and data as well.

Our cloud system will:

(a) Support efficient storage of encrypted sensitive data,

(b) Store, manage and query massive amounts of data,

(c) Support fine-grained access control and

(d) Support strong authentication.

This paper describes our approach to securing the cloud storage.

Fig 1: Cloud Computing

Till 2008 this cloud computing is shown as a network diagram, when it enhanced its services and resources over internet it termed as Cloud Computing. This cloud computing combines both activities like social networking sites and private group computing. But most of the time this cloud computing bothered to access online software applications, with data storage and power processing. It is the good way to enhance the capacity or dynamically adding capabilities without burden about new infrastructure, training or licensing software's. Due to its high speed and ubiquitous internet access the cloud user can access its services at any time and from anywhere.

Hsiao Ying Lin et al. For example, the email service is probably the most popular one. Users just use services without being concerned about how computation is done and storage is managed. In this paper, we focus on designing a cloud storage system by providing high security through the secret key sharing.

1.2 Cloud Storage System

In cloud computing the cloud storage system is advised as a large-scale distributed storage system that consists of many independent storage servers. Data robustness is a major requirement for storage systems. To store the data in cloud storage servers there were many proposals. The main way is to replicate the message and store a copy in each server; it provides robustness because it serves at least one server is active. Another ways is by using erasure coding technique, means the message was splits into pieces then encrypted.

The encrypted message again encoded as k symbols and then stored these different symbols in different servers; it makes more secure cloud storage. The storage server failure will occur due to error in code ward symbol. As long as the number of failure servers is under the tolerance threshold of the erasure code, the message can be recovered from the code word symbols stored in the available storage server's by the decoding process. The following figure illustrates the sample cloud storage system.

ISSN 22773061

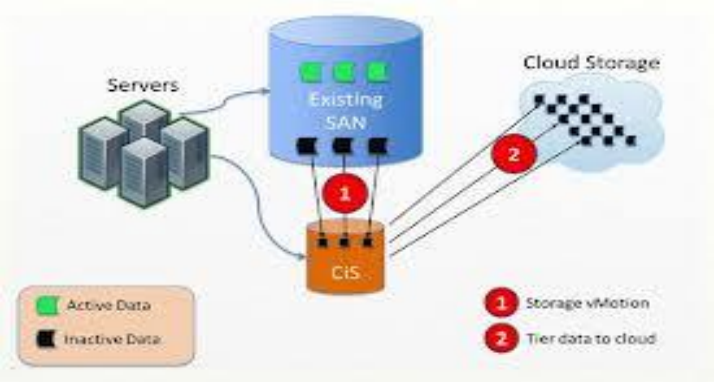


Fig 2: Cloud Storage System

This provides a tradeoff between the storage size and the tolerance threshold of failure servers. A decentralized erasure code is an erasure code that independently computes each code word symbol for a message. (Lin and TZENG, 2012) Thus, the encoding process for a message can be split into n parallel tasks of generating code word symbols.

In distributed storage system a decentralized erasure code is used. Each storage server identically computes their code ward symbol and stores it, when they receive the message symbols. This finishes the encoding and storing process. The recovery process is the same. The serious problem of data confidentiality is due to the data storage in third party's cloud. Before applying the erasure code method the user data will be encrypted and stored in storage servers, it provides strong confidentiality to user's data.

If any user wants to retrieve original data from cloud storage system, first he / she will retrieves the code word symbol, then decode that and then applies the decryption techniques with cryptographic keys. The following are the few problems in this: most of the computation must do by the user, so the network traffic is very high, the user only have to store the cryptographic keys if device is compromised, data storage and retrieving is too difficult for storage servers.

This threshold proxy re encryption technique has to maintain more servers. For example cloud storage servers, key servers and application servers. Even though this technique supports secure storage, retrieve and forwarding technique, it works under the public key pair only. If the key server and any one of storage server are compromised with third party, then the entire storage system loses its main functionalities.

1.3 Related Work

Based on ElGamal encryption techniques this Proxy re encryption concept introduced(Blaze et al., 1998). Based on the public key encryption technique there are several proxy re encryption techniques are proposed and those are in the identity based settings. Matsuo et al. proposed a hybrid proxy re-encryption scheme based on the ElGamal-type public key encryption system and Boneh–Boyen's identity-based encryption system. In 2008, bothLibert and Vergnaudare described a traceable proxy re-encryption system, in which a proxy who leaks its re-encryption key can be identified by the delegator. A variant of proxy re encryption called (C-PRE) conditional proxy re encryption was introduced by Tang and Weng et al. independently to control proxy at certain level.

Chu et al. introduced conditional proxy broadcast re-encryption (CPBRE) a generalized concept, and proposed a RCCA-secure CPBRE scheme. Shao et al. combined the primitives of proxy re-encryption and public key encryption with keyword search, and introduced the notion of proxy re-encryption with keyword search.

In 2006 there are two proxy re encryption techniques was proposed based on Identity based by Green and Ateniese. Those are: one is IND-Pr-ID-CPA secure and the other is IND-Pr-ID-CCA secure. Both are proven secure in the random oracle model under the decision a Ibilinear Diffie–Hellman (DBDH) assumption. CCA secure public key PRE scheme was proposed by Canetti and Hohenberger which is bidirectional and multi-use.

Key-privacy is a very useful attribution of PRE. In Ateniese et al. indicated that there are no PRE schemes satisfy the newly proposed attribution except theirs. Later, Fang et al. (2009) gave a construction of a conditional PRE to satisfy anonymous conditions.

Recently Wengetal. Revised concept on conditional PRE and constructed a more efficient scheme. By combining the both proxy re-encryption and public key encryption with keyword search, Shao et al. proposed a new cryptographic primitive called proxy re-encryption with keyword search (PRES) recently.

Hsiao-Ying Lin et al. (2012) proposed another new proxy re encryption technique called threshold proxy re encryption technique. In this, TPRE scheme integrates with a secured centralized erasure code to form a secure distributed storage system. This type of scheme supports operations like encoding in encrypted messages and forwarding operations over encrypted and encoded messages.

2. Preliminaries

This section we explains some preliminaries required to this paper. Here we explained two identity based encryption techniques as following:

2.1 Identity-based encryption:

An identity-based encryption scheme E is established by the following algorithms as a group (Setup, Key Generation, Encrypt, and Decrypt):

- Setup: Inputs k a security parameter, and outputs both the system's public parameters (parameter) which are distributed to users, and the master secret key (Master Secret Key) which is kept private to the Private Key Generator (PKG). The system parameters include a description of a finite message space M and a description of a cipher text space C.
- Key Generation: On input parameter, master secret key and an arbitrary idϵ {0, 1}*, the algorithm outputs a private key skid. Here id is an arbitrary string that will be used as a public-key, and skid is the corresponding private decryption key to the user with identity id.
- Encrypt: On input parameter, id ϵ {0, 1}*, and a message m ϵ M, the algorithm returns a cipher text c ϵ C.
- Decrypt: On input parameter, c ϵC, and private key skid, the algorithm returns m ϵ M or ⊥ (an invalid symbol represents arejection of the decryption).

We can say that an IBE scheme is consistent for any valid identity id and the corresponding private key skid which is generated by Key Generation, the following equation holds

Decrypt (parameter, Encrypt (parameter, id, m), skid = m, ∀m ϵ M.

The above explained algorithm is an identity based PRE with four main phases. In our proposed UMIB PRE two phases are added with existing four phases of IBPRE. The following algorithm illustrates the main theme of our algorithm to provide more secure cloud storage system and data forwarding as well.

2.2 Unidirectional Multiuse Proxy Re encryption:

This sub field explains few of the important uses of unidirectional proxy re encryption techniques:

- Unidirectional: Means there encryption key allows only from Alice to Bob and not from Bob to Alice.
- Prohibition of Interaction: to create a re encryption key, we require only Secret Key of Alice and Public Key of Bob, means Bob's secret key is not required.
- Non-interactive: For Re-encryption keys we won't allow third party, it can be done by Alice using Bob's public key. [Blaze et al. 1998].
- Authentic access: the re encrypted cipher text can decrypt by the Alice because she is the authentic user. In some cases, it is desirable to manage access to her re-encrypted cipher texts. This is an inherent feature of the Dodis–Ivan schemes the BBS scheme it can be done through adding some terms to the cipher text.
- Proxy invisibility: The proxy is transparent actually, but we allowed sender to encrypt message that can be opened by the intended recipient (first-level) or by any of the recipient's delegates (second-level). But they dint have knowledge to decrypt the first time encrypted cipher text.
- Key optimal: it means that the secret storage size of Bobis remains constant, regardless of how many delegations he accepts.
- Temporary: Dodis and Ivan [2003] suggested applying generic key-insulation techniques [Dodis et al. 2002, 2003, 2004] to their constructions to form schemes where Bob is only able to decrypt messages intended for Alice that were authored during some specific time period. This is an improvement over using current key-insulated schemes where the trusted server needs to individually interact with each user to help them update their master (and, therefore, delegation) secret keys [16].
- Collusion-resistance: even though Alice and proxy are working togetherthey dint no anything about Bob's secret key.

2.3 Unidirectional Multi-use Identity-based proxy re-encryption:

UMIB-PRE is the combination of unidirectional Multiuse PRE and identity based PRE techniques. An UMIB proxy re-encryption scheme is a set of algorithms (Setup, Key Generation, RKKey Generation, Encrypt, Reencrypt, and Decrypt) as follows:

- Setup (1k): On input a security parameter k, the algorithm outputs the system's public parameters (parameter) which are distributed to users and the master secret key (Master Secret Key) which is kept private to the PKG. The system parameters include a description of a finite message space M and a description of a cipher text space C.
- Key Generation (parameter, Master Secret Key, id). On input an identity id ϵ {0, 1}*and the master secret key (Master Secret Key), the algorithm outputs a decryption key sk corresponding to the user with identity id.

- Re encryption Key Generation(parameter, skidi, idj), (i≠j). On input a secret key skidi and identity idjϵ {0, 1}*, the algorithm outputs a unidirectional reencryption key from idi to idj as rkidi-idj.
- Encrypt (parameter, id, m). On input a set of public parameters, an identity id ϵ {0,1}*, and a plaintext m ϵ M, the algorithm outputs the first-level cipher text$c_{id}^{(1)}$, the encryption of m under identity id.
- Reencrypt (parameter, rkidi→idj,$c_{id}^{(l)}$), (l≥1). On input an lth -level cipher text $c_{id}^{(l)}$under identity idi, and a re-encryption key rkidi→idj, the algorithm outputs an (l+ 1)th-level re-encrypted cipher text $c_{idj}^{(l+1)}$, where $c_{idj}^{(l+1)}$is under identity idj.
- Decrypt (parameter, skid,$c_{id}^{(i)}$), (l≥1). The algorithm decrypts the l th-level cipher text$c_{id}^{(l)}$using the secret key skid, and outputsm ϵ M or ⊥.

We can say that the unidirectional and multi-use IB-PRE scheme is consistent for any valid identities idi, idj, (i ≠ j), their secret keys skidi,skidj, generated by Key Generation and the corresponding re-encryption key rkidi→idj , generated by RKKey Generation, and an lth-level (l≥1) cipher text$c_{idi}^{(l)}$ under identity idi output by Encrypt or Reencrypt, the following equations hold for∀ m ϵ M:

Decrypt (parameter, skidi, Encrypt (parameter,idi, m)) = m;

Decrypt (parameter,skidj, Reencrypt (parameter, rkidi→idj $c_{idi}^{(l)}$))=m, l≥1;

2.4 Integrity Checking Functionality

Integrity checking is another main functionality of cloud storage. The cloud user wants to check weather data is stored correctly or not in the cloud storage server. This concept explains the proof for secure storage of data in cloud servers. Audit must do on this issue on later by the user side. Nevertheless all of them consider the messages in the clear text form.

3. System Model

We presented the system model for our UMIB-PRE for secure cloud storage. In our UMIB PRE the system model comprises set of n storage servers S1 to Sn, Control server, Block Storage, proxy, users and m key servers K1 to Km. The storage services are provided by storage servers and key services are provided by key servers. These servers work based on their working nature. Our model consists of the following phases: system setup, key generation, re encryption key generation, encryption, data storage, data forward, proxy re encryption, data retrieval and decryption.

The following description shows the way of our system will work. The system administrator decides the system parameters and publishes them in the system setup phase. Systems public parameters are distributed to users. These parameters consist of cipher text space c and the finite message space M. and the master secret key which is kept private to PKG.

The second phase is the key generation phase. In this based on the input identity id and the master secret key the algorithm generates a decryption key corresponding to the user identity. The next phase is re encryption key generation, based on the secret key for particular identity, the algorithm produces the unidirectional re encryption key from idi to idj as rkidi-idj.

In this encryption phase the algorithms takes inputs set of public parameters called, identity id and message m and produces 1st level cipher text. This encryption can be done with m under the identity id. In this re encryption phase, the algorithm inputs 1st level cipher text under identity idi, and there encryption key rkidi-idj.

The algorithm outputs the (1+1) level re encrypted cipher text under the identity idj. The final phase is the decryption phase. In this the 1st level cipher text got decrypted with the secret key and out puts original message m.

4. Results and discussion

4.1 identity-based encryption scheme

In this RSA-OAEP, PSS cryptographic systems the random padding techniques are frequently used. OAEP first pads and then encrypts the plaintext, while PSS pads and then signs the message. In Bellare et al. one of the two OAEP schemes achieves a notion of plaintext-aware encryption. Therefore, we at first use random padding patterns to design an identity-based encryption scheme, which is the basis of our identity-based proxy re-encryption scheme described in the next subsection.

4.2 New construction of identity-based proxy re-encryption scheme

In this, we will use the above mentioned identity-based encryption scheme to create re-encryptable cipher texts and then model an identity-based proxy re-encryption scheme, which will be proven to be IND-PrID-CCA2 secure in the random oracle model. Moreover, Our IB-PRE scheme is unidirectional and multi-use.

Construction of a UM IB-PRE scheme was presented as an open problem by Green and Ateniese in Green et al. Multi-use is an important property for proxy re-encryptions. A multi-use PRE scheme permits the proxy (or proxies) to perform multiple re-encryptions on a single cipher text, e.g., re-encrypt from A to B, then re-encrypt the result cipher text from B to C, etc. The following diagram vividly describes this property. A cipher text intended for id1 can be converted to a cipher text for idl with the same message after (l - 1)-times re-encryption operations.

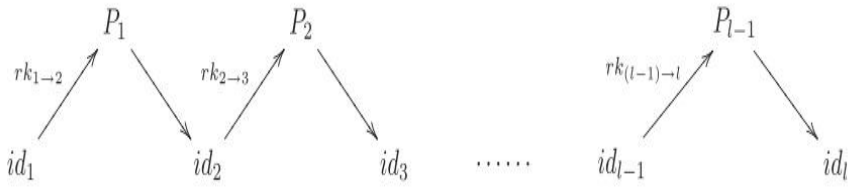


Fig 3: Example for UIB PRE

4.3 Analysis

(a) It is obvious that if the input to β is a DBDH tuple, then the challenge cipher text c* is a correct encryption of md under id*. Otherwise, c* is the encryption of a random element. Similarly, all elements given to β have the correct distribution.

(b) Probability that β does not abort. Let αi represents the value a generated by H1(idi).

i. On this (Key Generation, idi) query, if αi = 1, then β does not abort. Suppose that A makes query ex private key, Key Generation ion queries during the simulation, the probability that β does not abort is γqex.

ii. On this (rkKey Generation, idi, idj) query, if αi = 1, then β does not abort. Suppose that A makes qrk re-encryption key,Key Generationion queries during the simulation, the probability that β does not abort is γqrk.

iii. The query (reencrypt, idi, idj), if αi = 1, then β does not abort. Suppose that A makes q re-encryption queries during the simulation, the probability that β does not abort is c.

iv. (Decrypt,idi,$c_{id}^{(1)}$)In this,ifA has queried the private key of idi, then he can decrypt $c_{id}^{(l)}$ by himself. So without loss of generality, we suppose that A did not make an (Key Generation, idi) query before. If αi= 1, then β does not abort.

v. In the final stage, when A outputs its guess bit d', β does not abort if α* = 0. The probability that β does not abort in this case is (1 - γ). It is obvious that if B does not abort, the view of A in the simulation is identical to the view in the real attack.

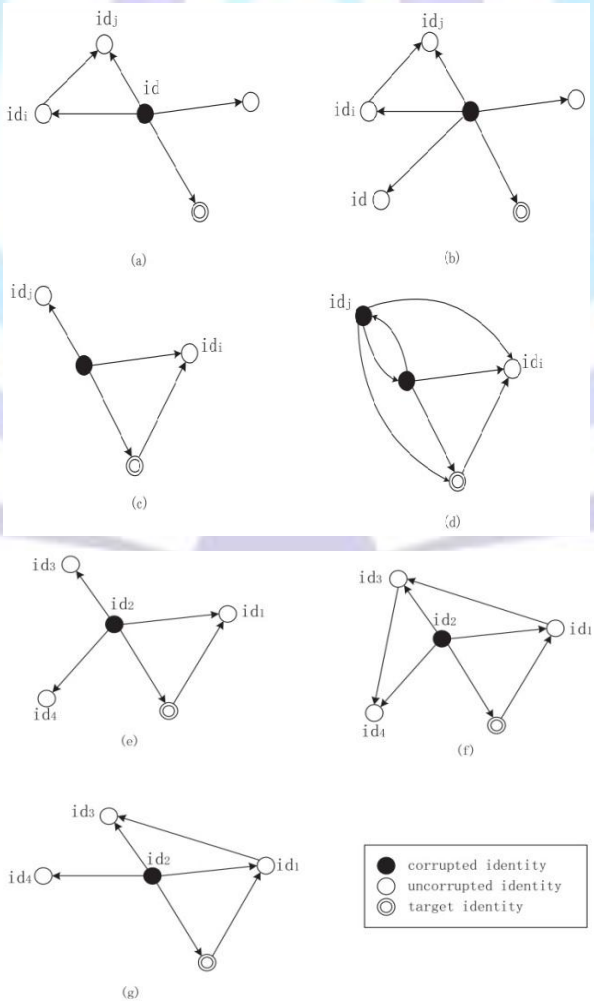


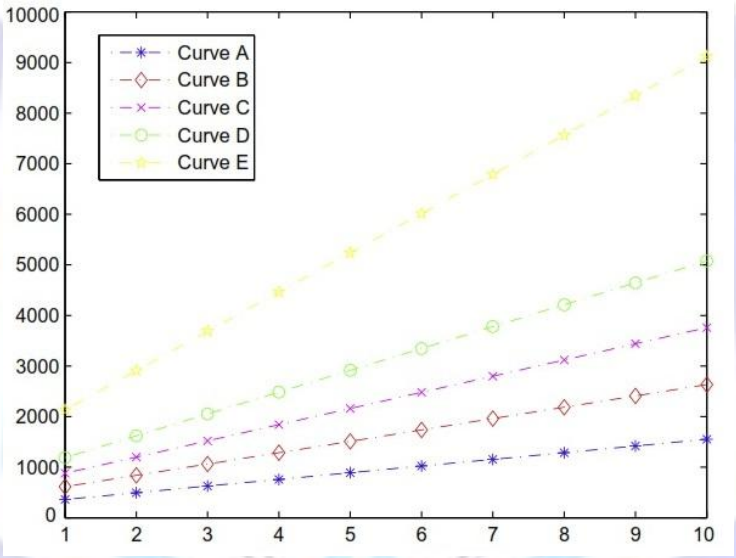
Fig 4: Multiuse directed graph model

4.4 Performance analysis

Our UMIB PRE performance got evaluated in this section. We do some performance analysis on our won UMIB-PRE. In this UMIB-PRE scheme performance analysis there are two aspects: the explanation of impact of different elliptic curves; discussion on the computation cost. Table 1 shows the processing time that measured for five MNT elliptic curves in milliseconds [18]. From the table the column SECC refers the parameter ECC Security of the bit size. This implementation was done on Windows XP machine with a Pentium 4 running at 2.40 GHz and 1GB RAM [18]. Schneier et al. a pairing operation is usually 2.5–3 times of an exponential operation. Here we ignored the hash computation, why because an exponential operation is approximately equal to 60 symmetric encryptions/decryptions, and a hashing operation is at least 10times faster than a symmetric encryption/decryption.

Curve	S_{ECC} (bits)	Tate pairing time (ms)
Curve A	160	33
Curve B	191	56
Curve C	221	80
Curve D	256	108
Curve E	307	194

Table 1: Cryptographic operations execution time



Graph 1: Computation cost of our UMIB-PRE

In the graph X-axis is the number of times of re encryptions and in Y – axis the total time for one process for our UMIB PRE. The above graph shows the different effects of five curves on our UMIB-PRE. When we have seen the implementation of all curves to check which curve is the most suitable one depends on different bandwidth or computational requirements Usually, Curve A with 160-bit is enough for most of the applications [2].

5. Conclusion

Our main intension is to build the secure cloud storage system, so first we will construct a cloud storage system, and then applied the security concerns. Up to now we used so called random padding techniques with identity based encryption to forward data securely. Existed IBE scheme is IND-ID-CCA2 secure in the random oracle model under the DBDH assumption. In this paper, we design an advanced IBE called Unidirectional and Multiuse IBE with several promising properties: secure in the sense of IND-PrID-CCA2 in the random oracle model under the DBDH assumption; unidirectional; and multi-use. Our UMIB-PRE scheme is a confirmative answer to the open problem presented by Green and Ateniese. Finally both of our IB-PRE and UMIB-PRE are proven to be secure for secure data forwarding in secure cloud storage.

References

[1]. Hsiao-Ying Lin and Wen-GueyTzeng, “A Secure Erasure Code-Based Cloud StorageSystem with Secure Data Forwarding” Vol 23, No 6, IEEE 2012, pp. 995-1003.

[2]. Hongbing Wang, Zhenfu Cao, Licheng Wang, “Multi-use and unidirectional identity-based proxy re-encryption schemes”, Elsevier 2010, pp. 4042-4059.

[3]. C. Dubnicki, L. Gryz, L. Heldt, M. Kaczmarczyk, W. Kilian, P.Strzelczak, J. Szczepkowski, C. Ungureanu, and M. Welnicki,"Hydrastor: A Scalable Secondary Storage," Proc. Seventh Conf. Fileand Storage Technologies (FAST), pp. 197-210, 2009.
[4]. C. Ungureanu, B. Atkin, A. Aranya, S. Gokhale, S. Rago, G.Calkowski, C. Dubnicki, and A. Bohra, "Hydrafs: A High-Throughput File System for the Hydrastor Content-AddressableStorage System," Proc. Eighth USENIX Conf. File and StorageTechnologies (FAST), p. 17, 2010.
[5]. W. Dong, F. Douglis, K. Li, H. Patterson, S. Reddy, and P. Shilane,"Tradeoffs in Scalable Data Routing for Deduplication Clusters,"Proc. Ninth USENIX Conf. File and Storage Technologies (FAST), p. 2,2011.
[6]. J.H. An, Y. Dodis, T. Rabin, On the security of joint signature and encryption, in: L.R. Knudsen (Ed.), EUROCRYPT, Lecture Notes in Computer Science, vol.2332, Springer, 2002, pp. 83–107.
[7]. G. Ateniese, K. Benson, S. Hohenberger, Key-private proxy re-encryption, in: M. Fischlin (Ed.), CT-RSA, Lecture Notes in Computer Science, vol. 5473,Springer, 2009, pp. 279–294.
[8]. G. Ateniese, K. Fu, M. Green, S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, in: NDSS, TheInternet Society, 2005.
[9]. G. Ateniese, K. Fu, M. Green, S. Hohenberger, Improved proxy re-encryption schemes with applications to secure distributed storage, ACM Trans.Inform. Syst. Secur. 9 (1) (2006) 1–30.
[10]. M. Bellare, P. Rogaway, Optimal asymmetric encryption, in: EUROCRYPT, 1994, pp. 92–111.
[11]. M. Bellare, P. Rogaway, The exact security of digital signatures – how to sign with RSA and Rabin, in: EUROCRYPT, 1996, pp. 399–416.
[12]. M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, in: EUROCRYPT, 1998, pp. 127–144.
[13]. D. Boneh, Simplified OAEP for the RSA and Rabin functions, in: [24], 2001, pp. 275–291.
[14]. D. Boneh, M.K. Franklin, Identity-based encryption from the weil pairing, in: [24], 2001, pp. 213–229.
[15]. D. Boneh, B. Lynn, H. Shacham, Short signatures from the weil pairing, J. Cryptol. 17 (4) (2004) 297–319.
[16]. HongbingWang,Zhenfu Cao, LichengWang"Multi-use and unidirectional identity-based proxy re-encryption schemes ".
[17]. Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, "Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, Vol. 9, No. 1, February 2006.
[18]. D. Page, N.P. Smart, F. Vercauteren, A comparison of MNT curves and supersingular curves, Appl. Algebr. Eng., Commun. Comput. 17 (5) (2006) 379–392.
[19]. B. Schneier, Applied Cryptography, Protocols, Algorithms, and Source Code in C, second ed., John Wiley and Sons Inc., 1996.

Author Profiles

Mr. P. Radha Krishna Reddy received his Bachelor of Science in Computer Science from Sri Venkateswara University-Tirupati in 2007, Master of Science in Computer science from Sri Venkateswara University-Tirupati in 2009. Pursuing Master of Technology in Computer Science and Engineering from VITS, Jawaharlal Nehru Technological University-Anantapur. This work is done for his M Tech CSE dissertation. He has 2+ years of teaching experience and published journals on different fields of Computer Science.

Mr.S.Sivaramaiah received his MCA from Sri Venkateswara University-Tirupati, andM.Tech (CSE) from Acharya Nagarjuna University. He has 7 years of teaching Experience, and working as Asst Prof in Vaagdevi Institute of Technology and Sciences, JNTU-Anantapur.

Mr.U.Sesadri received his M.Sc (CS) from SriVenkateswara University-Tirupati, M.Tech (CSE) from Satyabhama University. Working as HOD in CSE in Vaagdevi Institute of Technology and Sciences, under JNTU-Anantapur and have 10yearsofexperience.