Key-Aggregate Proxy Re-Encryption With Dynamic Condition Generation Using Multilinear Map

Mrs. Srilatha Puli[1*], Kandhi Vaman Reddy[2], Kankanala Vinay[3], Mughaisa Fatima[4], Choppara Ramya Sree[5]

[1*]Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,Email: srilatha.puli@sreyas.ac.in
[2]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. Vamanreddy12389@gmail.com
[3]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. Vinnureddy.k@gmail.com
[4]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. Mughaisafatima21@gmail.com
[5]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India. Email: Chopparamyasree89@gmail.com

***Corresponding Author:** Mrs. Srilatha Puli
*Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,Email: srilatha.puli@sreyas.ac.in

Abstract:
The rapid growth of cloud computing and the increasing demand for secure data sharing have brought forth the need for efficient and flexible encryption schemes. Key-Aggregate Proxy Re-Encryption (KAPRE) is a cryptographic primitive that enables a data owner to delegate decryption rights to multiple proxies while preserving fine-grained access control over the shared data. This paper proposes a novel approach to KAPRE by incorporating dynamic condition generation using multilinear map cryptography. The main objective of this research is to develop an enhanced KAPRE scheme that allows the data owner to dynamically generate access conditions for the proxies, thereby providing more flexible and fine-grained control over the shared data. This is achieved by leveraging the properties of multilinear maps, a powerful tool in modern cryptography. The proposed scheme employs multilinear maps to enable the data owner to generate dynamic access policies based on various attributes and conditions. The proxies are equipped with re-encryption keys that can transform the ciphertext encrypted under the data owner's public key into a ciphertext that can be decrypted by authorized users satisfying the specified access conditions.To ensure the security and efficiency of the proposed scheme, this paper addresses several key challenges, including secure multilinear map construction, access policy generation, re-encryption key management, and efficient decryption of the shared data. Furthermore, the paper presents a comprehensive security analysis, evaluating the proposed scheme against various cryptographic attacks and discussing its resistance to known vulnerabilities. The performance of the scheme is also evaluated through extensive simulations, demonstrating its efficiency and scalability.The results of this research contribute to the field of secure data sharing in cloud environments by providing an advanced KAPRE scheme that offers enhanced flexibility and fine-grained control over data access. The proposed scheme has the potential to benefit various applications that require secure and efficient data sharing, such as collaborative environments, healthcare systems, and IoT platforms.

Keywords *– Key-Aggregate Proxy Re-Encryption,Dynamic Condition Generation, Multilinear Map, Secure Data Sharing, Cloud Computing, Fine-Grained Access Control.*

1. INTRODUCTION

With the development of modern technology and the growing accessibility of the internet, the age of internet making our lives more efficient and convenient has come. Hundreds of thousands of files are stored in cloud storages. To ensure that data can be stored in the cloud securely, most of the users encrypt the files before uploading them to the cloud. However, a problem appears when people want to share their files under encrypted forms with other users. A trivial solution is that the owner of the file must share the encryption key with the file receivers also. Obviously, this will violate the security due to the leak of the encryption key. In order to solve this situation, Blaze et al. first introduced the concept called "Proxy ReEncryption (PRE)" in 1998.

The main idea is to introduce a "proxy" who can convert an encryption for one to another through a valid re-encryption key.
Proxy re-encryption can be divided into four categories.
1) Single-hop: It means that a ciphertext can only be reencrypted once.
2) Multi-hop: It means that a ciphertext can be re-encrypted multiple times. (i.e. A ciphertext can be re-encrypted from Alice to Bob, and the re-encrypted ciphertext can be further re-encrypted to Carol, and so on.)

3) Uni-directional: A proxy can only re-encrypt Alice’s ciphertexts into Bob’s, but Bob’s ciphertexts cannot be re-encrypted into Alice’s.
4) Bi-directional: A proxy can re-encrypt Alice’s ciphertexts into Bob’s, and vice versa.

With the continuous development of cloud computing technology, a new kind of data storage model called cloud storage has attracted great attention. Derived from cloud computing, cloud storage can provide online storage space through the network [1]. With the advantage of low cost, easy utilizing, and high scalability, it can meet the needs of the mass data storage and provide data sharing service, which has become the important area in the data storage technology. After requesting the storage service from cloud service providers, enterprises or individuals store a large amount of data to the cloud server, greatly reducing the burden of the local hardware infrastructure and saving the local storage overhead. What is more, its function of data sharing is regarded as very important for multiuser cloud computing environment. When data owners outsource their data in the server and want to share these data with other users, they can adopt techniques to delegate permission to these users. By this way, the legitimate users can have access to corresponding data from the cloud server so as to achieve the process of data sharing However, when cloud storage brings great convenience for users dealing with large-scale data, it also brings new security issues and challenges [2]. Because the cloud server is not completely trusted, enterprises or individuals will lose absolute control over the data outsourced to the cloud data, which brings the worries about data security and privacy protection. So for these data, such as how to use encryption scheme to ensure the cloud security and how to protect the data privacy, realize effective data sharing, and reduce the user key management cost as much as possible, keyaggregate cryptosystem is brought forward at this moment. In such cryptosystem, user’s private keys can be aggregated together to be a single key and only using the single key can user decrypt the corresponding multiple encrypted files, which simplifies the user’s key management. It also grants different decryption access for different users and can be applied to the data sharing in cloud flexibly. Meanwhile, since user’s access changed dynamically and frequently in the cloud environment, how to realize user’s access control and revocation become vital problems to be solved. For example, when an employee leaves his company, he will no longer have permission to the company’s internal data. So, in order to meet the dynamic change of user access, it is necessary to consider the problem of user revocation.

Therefore, according to the characteristics of cloud storage, the research and establishment of an efficient and secure revocable key-aggregate encryption scheme is very necessary and urgent, which has important theoretical significance and application value.

2. LITERATURE REVIEW

In recent years, it has become a crucial problem to realize secure and effective data sharing, as well as reducing the key management costs in the cloud environment. How to reduce the number of keys that users have to save, thus simplifying the key management problems effectively, has been a hot research topic. In existing research results, they can mainly be divided into four kinds in reducing the cost of the key management: hierarchical key management scheme, key compression scheme based on symmetric encryption, identity-based key compression scheme, and other related solutions In cloud storage, the hierarchical key management scheme generally utilizes tree structure, where the key of each nonleaf node can generate keys of its child nodes. And users only need to save the corresponding ancestor nodes, effectively simplifying the key management. This technology was first proposed by Akl and Taylor and later has been applied to the cloud environment with the rise of cloud computing. For example, Ateniese et al. put forward a predefined hierarchical key management scheme based on the logical key tree. However, the main drawback of hierarchical key management scheme was that only under certain conditions can it achieve effective key compression. This was because the node key can only access to the subtree of the node, if authorized files were from different branches, which in turn would increase the number of users’ private keys. So its key compression was limited; only when sharing all the documents from the same branch in the tree, it could achieve the effective compression of private key In order to solve the issue that it needs to transport a large number of keys in the broadcast encryption scenario, Benaloh et al. proposed a key compression scheme based on symmetric encryption. Its basic method is to split the entire ciphertext space into finite sets and generate a constantsize key corresponding to each of these sets, so as to realize the effect of key compression. Other schemes were also symmetrical encryption schemes trying to reduce the key size. Since these schemes were set in the environment of symmetric encryption, which required sharing a symmetric key through secure channel, their application scenarios were greatly limited in the cloud environment.

As Shamir proposed the concept of identity-based encryption (IBE) and then Boneh and Franklin put forward the first practical IBE scheme using bilinear pairings, it brought out the research of identity-based key compression scheme. Guo et al. presented a multi-identity single key decryption scheme and proved its security in the random oracle model. In their scheme, when user adopted different identities as the public key in different scenarios, for example, user had more than one email address; it only needed to store a private key to decrypt multiple encrypted messages from different companies, remarkably cutting down the cost of the user key management. Then made improvements on the efficiency and achieved adaptive chosen-ciphertext security in the standard model. But in these schemes, key compression was restricted, which required all the keys from different identity divisions, and the length of ciphertext and public parameters were linearly related to the maximum number of keys that can be aggregated, which increased the overhead of storage and transmission.

Sahai and Waters proposed a fuzzy identity-based encryption (FIBE) scheme to take users' biometric information as their identities, so that user's identity was no longer a single one but was made up of several attributes. It allowed a private key to decrypt multiple ciphertexts and was proved to be secure in the standard model. However, this scheme required the ciphertext to be encrypted by identity that met certain conditions, so it could not achieve the flexible key compression.

Other relevant solutions include the attribute-based encryption (ABE) and proxy reencryption (PRE). Waters presented an ABE scheme that its private key was associated with the strategy, and ciphertext was associated with attributes and could decrypt when strategy matched with attributes. In their scheme, however, the length of private key was linearly related to the leaf nodes in the strategy access tree. Li et al. Applied ABE to share keys in group users, but the main concern was to resist collusion attacks, rather than key compression. Canetti and Hohenberger put forward PRE scheme using the thought of transformation to turn the original ciphertext into the ciphertext encrypted by the user's public key. However, such technology is essentially aimed at transferring the secure key storage to the cloud proxy server. In addition, a key management scheme based on secret sharing was proposed suitable for wireless sensor networks.

Recently, Chu et al. first put forward the concept of key-aggregate cryptosystem (KAC) and constructed the first key-aggregate encryption scheme applied to data sharing in the cloud environment flexibly. The scheme was set in public key cryptosystem and it could aggregate users' private key to be a single one, so that users only stored this aggregated key to decrypt multiple files. Most importantly, its aggregation could be achieved without conditions and kept the length of ciphertext in constant-size. However, the length of system parameters in their scheme was linearly related to the maximum number of files, and it did not provide a specific security proof. Soon afterwards, the thought of keyaggregate cryptosystem was adopted, such as Dang et al. who applied the key-aggregate cryptosystem in the wireless sensor network and proposed a fine-grained sharing scheme to the encrypted senor data. Sikhar et al. proposed a dynamic key-aggregate encryption scheme to realize the user revocation. But one of its imitations was that once user revocation occurred, all legitimate users needed to update their private keys, which brought expensive overhead of key update.

3. METHODOLOGY

In order to solve the key management problems and realize dynamic access control during data sharing more effectively, this paper has been focused on the study of revocable key-aggregate cryptosystem in cloud. Its main contribution shows the following:

(1) According to the characteristics of the key-aggregate cryptosystem and the needs for user revocation, this paper first makes formal definition about the revocable key-aggregate cryptosystem.

(2) Combining the subset-cover framework, this paper puts forward an efficient revocable key-aggregate encryption scheme based on multilinear maps, realizing the user's access control and revocation. Our construction not only has the characteristics of key aggregation, which simplifies the user's key management effectively, but also can delegate different users with different decryption permission and achieve revocation of user access rights, realizing the flexible access control effectively.

(3) Compared with the existing schemes, this paper analyzes the related performance for the proposed scheme. It indicates that our scheme not only keeps the users' secret key and the ciphertext in constantsize, but also reduces the length of system parameters to $O(\log N)$, where N is the maximum number of files in the system, thus saving the cost of storage and transmission efficiently. By updating ciphertext via the cloud servers, the proposed scheme realizes the user permissions revocation while legitimate users do not need to update their private keys. What is more, it provides a verification mechanism to ensure user revocation executed correctly.

(4) Lastly, security analysis shows that the proposed scheme is proved to be selective chosen-plaintext security based on Generalized DHDHE assumption in the standard model. In addition, we discuss a solution to extend our basic scheme to solve the rapid growing number of files in the cloud environment.

MODULES:

The following modules were created to carry out the aforementioned project.

It consists of three entities:

1. Cloud service provider (CSP),
2. Data owner (DO)
3. Data User

4. IMPLEMENTATION

In this section, we adopt an asymmetric multilinear map to design a key-aggregate proxy re-encryption. Our scheme is motivated from Chen et al.'s scheme. In their scheme, the number of types is corresponding to the length of the public key of a user, and thus it should be fixed at the KeyGen phase. In our scheme, we apply multi-linear maps to solve the problem. Though the number of conditions in our scheme is also fixed, it can be exponentially large.

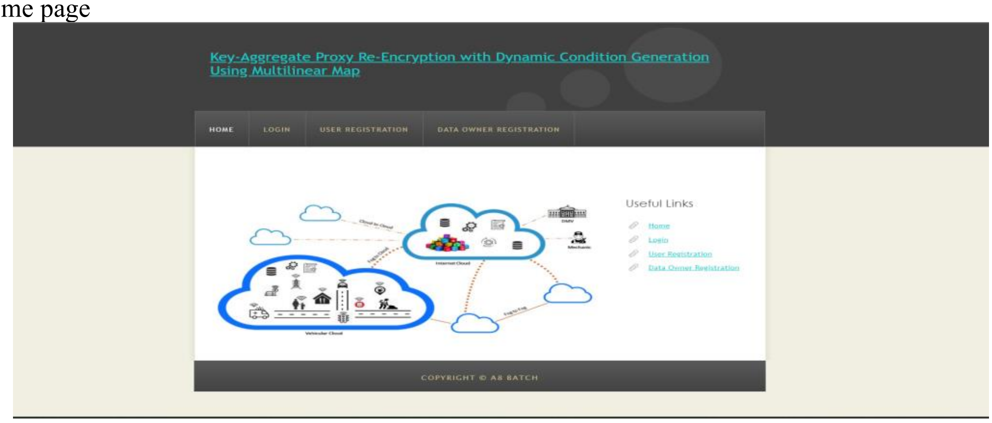
We present a key-aggregate proxy reencryption from multilinear maps which can dynamically generate conditions. It includes eight algorithms: Setup, KeyGen, ReKeyGen, Enc2, Enc1, ReEnc, Dec2, Dec1.

We applied multilinear maps instead of bilinear maps to a key-aggregate proxy re-encryption (KAPRE) scheme such that the proposed scheme has a short public parameter, while preserving constant-size re-encryption keys. The space complexities of a re-encryption key and the public parameter are O(N) and O(logN), respectively, where N is the maximum number of conditions in the proposed scheme. Another advantage of the proposed scheme is that, we can add any conditions even after the setup phase, which makes it more flexible and practical.

This paper proposes a revocable key-aggregate encryption scheme and proves its security in the standard model. The main thought of the scheme lies in constructing the ciphertext and the private key. The ciphertext of the new scheme includes not only the file index, but also the user revocation set, realizing the user revocable directly. At the same time, the private key is correspondingly divided into two parts. One is the aggregation of the file index set, and the other is the aggregation of the path set for each user, so as to realize the user's key aggregation effectively. Through the above method, only the legitimate users have access to the appropriate file, realizing the file access control function in the system effectively. This new scheme achieves the ciphertext updating through the cloud servers to save the computational overhead of data owner; when the user revocation occurs, nonrevoked user does not need to update his private key, greatly reducing the key update expensive cost and the burden of key delegate authority; because the cloud server is not completely trusted, we consider to provide a verification mechanism for the scheme, so that the data owner can validate the updated ciphertext to make sure the user revocation is carried out correctly.

4. EXPERIMENTAL RESULTS

This is the home page



Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map

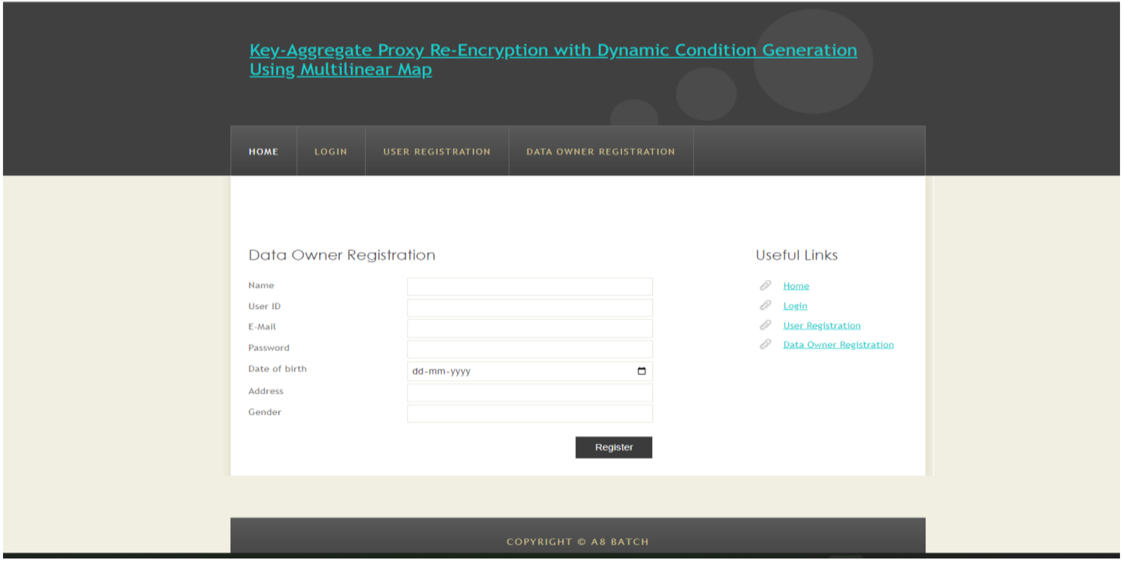
Useful Links

- Home
- Login
- User Registration
- Data Owner Registration

COPYRIGHT © A8 BATCH

Screenshot 8.1.1 Home page

This page lets the data owner register itself



Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map

Data Owner Registration

Name

User ID

E-Mail

Password

Date of birth dd-mm-yyyy

Address

Gender

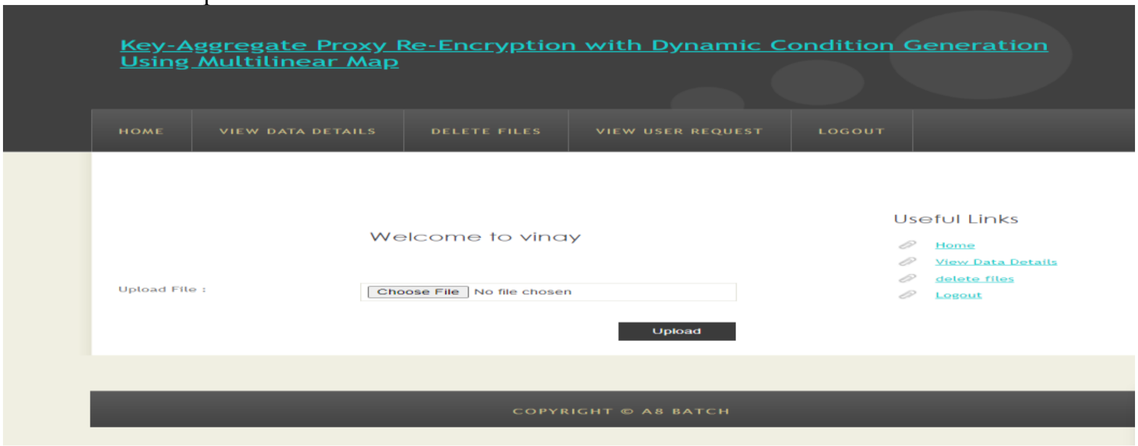
Useful Links

- Home
- Login
- User Registration
- Data Owner Registration

COPYRIGHT © A8 BATCH

Screenshot 8.1.2 Data owner register page

Now the data owner can upload the file.



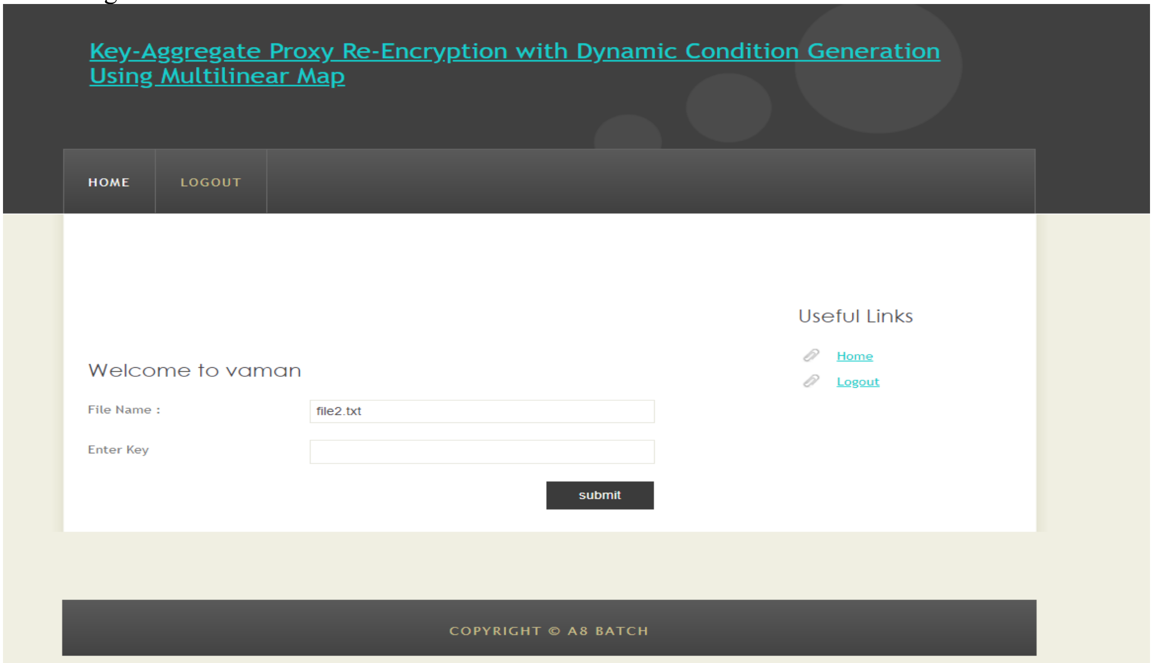
Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map

Welcome to vinay

Upload File : No file chosen

Screenshot 8.1.3 upload file

The data owner gives the file name.



Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map

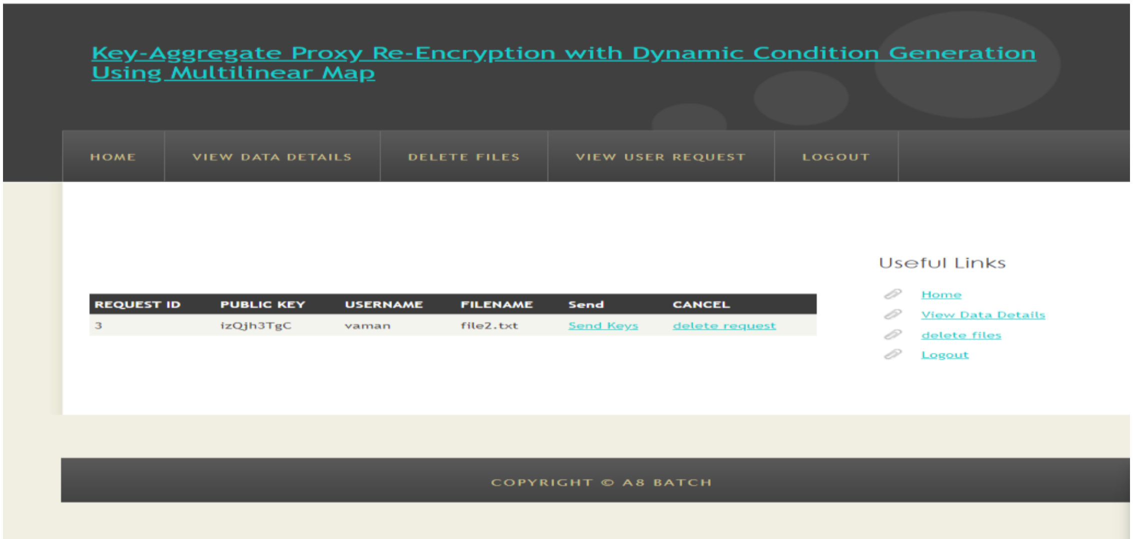
Welcome to vaman

File Name : file2.txt

Enter Key

Screenshot 8.1.4 data owner gives the file namelist of scree

Now the key will appear to the data owner and appear the request from the user.

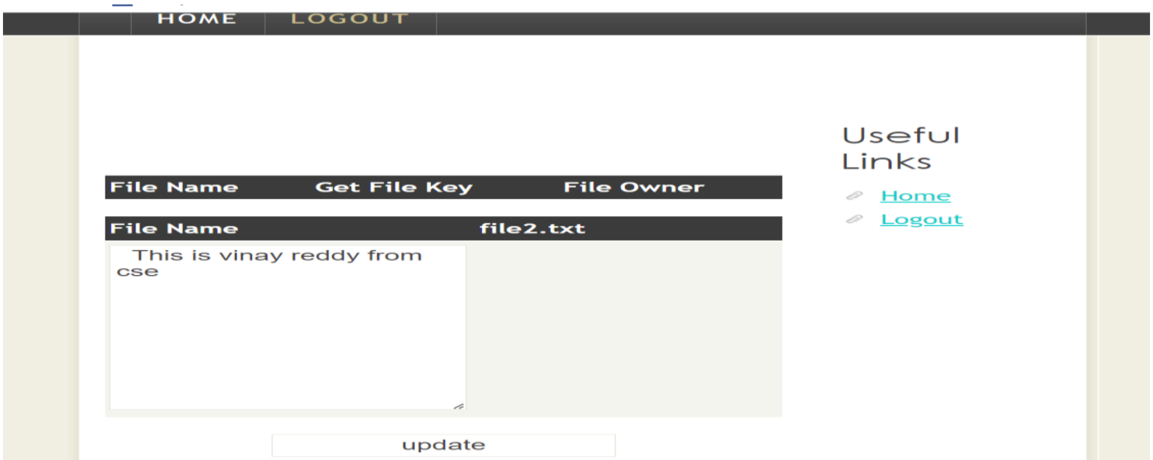


Key-Aggregate Proxy Re-Encryption with Dynamic Condition Generation Using Multilinear Map

REQUEST ID	PUBLIC KEY	USERNAME	FILENAME	Send	CANCEL
3	izQjh3TgC	vaman	file2.txt	Send Keys	delete request

Screenshot 8.1.5 Data owner gets request

Now the user can edit or delete the data by sharing the key from the data owner.



File Name	Get File Key	File Owner

File Name	file2.txt
This is vinay reddy from cse	

Screenshot 8.1.6 Authorized user editing the file

6. CONCLUSION

We applied multilinear maps instead of bilinear maps to a key-aggregate proxy re-encryption (KAPRE) scheme such that the proposed scheme has a short public parameter, while preserving constant-size re-encryption keys. The space complexities of a re-encryption key and the public parameter O(N) and O(logN), respectively, where N is the maximum number of conditions in the proposed scheme. Another advantage of the proposed scheme is that, we can add any conditions even after the setup phase, which makes it more flexible and practical.

REFERENCES

1. M. Blaze, G. Bleumer, And M. Strauss, “Divertible Protocols And Atomic Proxy Cryptography,” In International Conference On The Theory And Applications Of Cryptographic Techniques. Springer, 1998, Pp. 127– 144.
2. J. Weng, R. H. Deng, X. Ding, C.-K. Chu, And J. Lai, “Conditional Proxy Re-Encryption Secure Against Chosen-Ciphertext Attack,” In Proceedings Of The 4th International Symposium On Information, Computer, And Communications Security. Acm, 2009, Pp. 322–332.
3. W.-H. Chen, C.-I. Fan, And Y.-F. Tseng, “Efficient Key-Aggregate Proxy Re-Encryption For Secure Data Sharing In Clouds,” In 2018 Ieee Conference On Dependable And Secure Computing (Dsc), Dec 2018,

D. Boneh And A. Silverberg, “Applications Of Multilinear Forms To Cryptography,” Contemporary Mathematics, Vol. 324, No. 1, Pp. 71–90, 2003.

4. S. Garg, C. Gentry, And S. Halevi, “Candidate Multilinear Maps From Ideal Lattices,” In Annual International Conference On The Theory And Applications Of Cryptographic Techniques. Springer, 2013, Pp. 1–17.
5. J.-S. Coron, T. Lepoint, And M. Tibouchi, “Practical Multilinear Maps Over The Integers,” In Advances In Cryptology–Crypto 2013. Springer, 2013, Pp. 476–493.
6. C. Gu, “Multilinear Maps Via Secret Ring,” Cryptology Eprint Archive, Report 2018/312, 2018, Https://Eprint.Iacr.Org/2018/312.
7. M. R. Albrecht, P. Farshim, S. Han, D. Hofheinz, E. Larraia, And K. G. Paterson, “Multilinear Maps From Obfuscation,” Journal Of Cryptology, Pp. 1–34, 2020.
8. Srilatha Puli, A Machine Learning Model For Air Quality Prediction For Smart Cities, Design Engineering || Issn: 0011-9342 | Year 2021 - Issue: 9 | Pages: 18090 – 18104
9. Srilatha Puli, Quality Risk Analysis For Sustainable Smart Water Supply Using Data Perception, International Journal Of Health Sciences Issn 2550-6978 E-Issn 2550-696x © 2022, Https://Doi.Org/10.53730/Ijhs.V6ns5.9826, 18 June 2022
10. Srilatha Puli, Urban Street Cleanliness, Journal Of Algebraic Statistics Volume 13, No. 3, 2022, P. 547-552, Https://Publishoa.Com, Issn: 1309-3452
11. Srilatha Puli, Self-Annihilation Ideation Detection, Neuroquantology | June 2022 | Volume 20 | Issue 6 | Page 7229-7239 | Doi: 10.14704/Nq.2022.20.6.Nq22727
12. Srilatha Puli, Crime Analysis Using Machine Learning, Ymer|| Issn: 0044-0477, April 2022
13. Srilatha Puli, N-Grams Assisted Youtube Spam Comment Detection, Ymer || Issn: 0044-0477, April 2022
14. Srilatha Puli, Analysis Of Brand Popularity Using Big Data And Twitter, Ymer|| Issn: 0044-0477, April 2022
15. Srilatha Puli, Cyber Threat Detection Based On Artificial Neural Networks Using Event Profiles,The International Journal Of Analytical And Experimental Modal Analysis, Issn No:0886-9367
16. Srilatha Puli, Face Mask Monitoring System, The International Journal Of Analytical And Experimental Modal Analysis, Issn No:0886-9367
17. Srilatha Puli, Iot Based Smart Door Lock Surveillance System Using Security Sensors, Advanced Science Letters E-Issn:1936-7317
18. Srilatha Puli, Safety Alerting System For Drowsy Driver, 9th International Conference On Innovations In Electronics & Communication Engineering (Iciece-2021), Page – 40

19. N. Swapna Suhasini, Srilatha Puli, Big Data Analytics For Malware Detection In A Virtualized Framework, Journal Of Critical Reviews, Issn:2394-5125 Vol.7, Issue 14, July – 2020
20. Srilatha Puli, Block Chain Based Certificate Validation, International Journal Of Science And Research (Ijsr), Issn: 2319-7064 Sjif (2022): 7.942, Volume 11 Issue 12, December 2022, Paper Id: Sr221219113003, Doi: 10.21275/Sr221219113003, Www.Ijsr.Net
21. Mrs. Srilatha Puli, Energy Efficient Teaching-Learning-Based Optimization For The Discrete Routing Problem In Wireless Sensor Network, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022.
22. Mrs. Srilatha Puli, A Hybrid Block Chain-Based Identity Authentication Scheme For Multi- Wsn, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022
23. Mrs. Srilatha Puli, Implementation Of A Secured Watermarking Mechanism Based On Cryptography And Bit Pairs Matching, International Journal Of Early Childhood Special Education (Int-Jecs) Doi: 10.48047/Intjecse/V14i7.296 Issn: 1308-5581 Vol 14, Issue 07 2022
24. Mrs. S.Sunitha, Mrs. Srilatha Puli, Multilevel Data Concealing Technique Using Steganography And Visual Cryptography, International Journal Of Early Childhood Special Education (Int-Jecse) Doi:10.48047/Intjecse/V15i1.1 Issn: 1308-5581 Vol 15, Issue 01 2023
25. Mrs. Srilatha Puli, Blood Bank Management Donation And Automation, Specialusis Ugdymas/Special Education 2022 1 (43), Https://Www.Sumc.Lt/Index.Php/Se/Article/View/1995
26. N. S. Suhasini And S. Puli, "Big Data Analytics In Cloud Computing," 2021 Sixth International Conference On Image Information Processing (Iciip), Shimla, India, 2021, Pp. 320-325, Doi: 10.1109/Iciip53038.2021.9702705.
27. Surarapu Sunitha, Blockchain-Based Access Control System For Cloud Storage, Ymer || Issn: 0044-0477, April 2022
28. Surarapu Sunitha, Artificial Intelligence Support For Cloud Computing Intrusion , Deep-Cloud Issues, Solid Stage Technology, Volume:63, Issue:2s, Publication-2020
29. Surarapu Sunitha, Cryptocurrency Price Analysis Using Artificial Intelligence, Journal Of Algebraic Statistics Volume 13, No. 3, 2022, P. 486-493 Https://Publishoa.Com Issn: 1309-3452
30. Surarapu Sunitha, An Empirical Study On Security Issues And Mitigation Techniques In Opportunities Networks, Think India Journal, Issn:0971-1260, Vol-22, Issue-41, December-2019
31. Surarapu Sunitha, A Hybrid Block Chain-Based Identity Authentication Scheme For Multi-Wsn, International Journal Of Early Childhood Special Education, Issn:1308-5581, Vol 14, Issue July-2022
32. Sunitha Surarapu, Cryptocurrency Price Prediction Using Neural Networks, Deep Learning And Machine Learning , International Journal For Innovative Engineering And Management Research, Issn:2456-5083, Volume 12, Issue 05 May 2023, Pages:408-417
33. Sunitha Surarapu, Multilevel Data Concealing Technique Using Steganography And Visual Cryptography, International Journal Of Early Childhood Special Education, Volume 15, Issn:1308-5581, Iisue January 2023