IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

Efficient Dynamic Auditing for Cloud Storage Security and Integrity of Data in Cloud

Mr.K.R.Mohan Raj , Aarthy S K, Abinaya Khataukar S, Krithika K

Assistant Professor – II, Department of Information Technology, Velammal Engineering College, Chennai, India

Department of Information Technology, Velammal Engineering College, Chennai, India

Department of Information Technology, Velammal Engineering College, Chennai, India

Department of Information Technology, Velammal Engineering College, Chennai, India

ABSTRACT : The cloud security is one of the important roles in cloud, with which we can preserve our data into cloud storage. More and more clients store their data to PCS (public cloud servers) everyday with the rapid development in cloud computing. Cloud storage services allow users to outsource their data to cloud servers to save local data storage costs.Multiple verification tasks from different users can be performed efficiently by the auditor and the cloud-stored data can be updated dynamically. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. We are using our own auditing system based on the token generation. Using this key generation technique , we can compare the key values from original keys we can find out the changes about the file.

Not only stored also the content will be encrypted in the cloud server. Encryption is done by using two symmetric encryption algorithms- AES and blowfish algorithm. To view the file stored in cloud, users need to first decrypt the files and also combine the split files from three different locations. This is not possible by anyone. Users can download the files from the server with file owner permission. At the time of download , a is key generated (code based key generation) and it will be sent to the file owner. User can download the file but to use file owner permission is necessary.

KEYWORDS: AES, blowfish, token generation, symmetric encryption, key generation.

I. INTRODUCTION

Cloud computing in simple terms is providing a service like data storage, resources, software to the user over the internet remotely by the CSPs (Cloud Service Provider). To access these services, all user needs is a stable internet connection. User only pays for the service they use. Cloud computing was referenced as early as 1996 and became popularized in 2006. Several features like ubiquity, resource pooling, elasticity, on-demand self-service, scalability etc. have made cloud popular worldwide and is hence used by several organizations. We as users several cloud applications on a day-to-day basis. Most commonly used cloud services include Gmail, Microsoft word etc., IP traffic in Cloud services is expected to grow up to 19.5 zettabytes in 2021.In 2020, the market is expected to demonstrate the growth rate of 17%[1].

There are four types of cloud deployment models. They are public cloud, private cloud, hybrid cloud and community cloud. Public cloud as the name suggests is available for access to the public. Anyone with an account can access the data in the public cloud. Private cloud on the other hand means data access is very much restricted. Users can access only the data that is available to them. Hybrid cloud is a combination of both public and private cloud. Certain data is available to everyone whereas certain data is available only to users who have access to it. Community cloud is used when data needs to be shared only with a certain group of people. Different deployment models have varying levels of security associated with them.

There are several deployment models available but the three standard deployment models as defined by the NIST are Infrastructure as a service (IAAS), Platform as a service (PAAS), Software as a service (SAAS). In IAAS, most of the cloud stack has to be configured by the user. In PAAS, user needs to configure data and the application while the rest of the cloud stack is configured by the CSP itself. In SAAS, the entire software is delivered to the user over the internet. User only has to use this software. Other deployment models include Mobile-backend as a service (MbAAS), Functions as a service (FAAS) etc.,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

Popular providers of cloud service are Google, Microsoft, Amazon, IBM and Salesforce. There are several benefits associated with cloud services such as ubiquity, pay only for the amount of service we use, easy updates, easy access for users, affordable services etc.,

While there are several benefits which attracts the organizations, there are several disadvantages of using cloud as well. The first and the foremost issue associated with cloud is security. Several attacks are being done on the cloud on everyday basis. Protecting the data stored in the cloud and its services is a must with the rapid increase in the usage of cloud. Data that is stored in cloud is protecting by using cryptographic techniques such as encryption and integrity checking.

Encryption is a process in which text in readable format is converted to ciphertext using a key. Decryption is the reverse process of encryption. Using the key, ciphertext is converted back to readable text format. There are two types of encryption schemes- Symmetric encryption in which same key is used for both encryption and decryption and Asymmetric encryption in which different keys are used encryption and decryption. Encryption ensures confidentiality of data. Integrity is ensuring that data remains unaltered by unauthorized people. This is done by various checking schemes most common one being checksum method. Checksum of the data is stored and the checksum is checked again when the data is accessed. If the data is modified then the checksum will be different.

Authentication method also plays an important role in the security of cloud account. Two-factor authentication is followed in our proposed model which is most effective authentication to date. In two-factor authentication, user uses their username and password to login after which an OTP (One Time Password) is sent to their registered mail account which will be further used to verify the authenticity of the user. Data that is stored in the server is split into three parts and stored making it more difficult for hackers to gain the whole decrypted information.

II. LITERATURE REVIEW

J. Li, H. Yan and Y. Zhang [1]have proposed that the certificate is not needed. A new RDPC (remote data possession checking) protocol for checking the integrity of data shared among a group. The advantage of this method is that the issue of key escrow is eliminated since identity based encryption is not used. Whereas the disadvantage is Users in the same group can share data with each other, and access and modify the shared data leading to integrity issues.

Zhang Y, Yu J, Hao R, Wang C, Ren K[2] have produced a novel storage auditing scheme that achieves high efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud .The advantage is that integrity auditing of the revoked user's data can still be correctly performed when the authenticators are not updated. The disadvantage is that it leads to key escrow problem.

Chen, Y., Liu, H., Wang, B depict[3] in their paper which proposes a new threshold hybrid encryption for integrity auditing method without trusted centre. The proposed method is developed based on the Advanced Encryption Standard (AES) and the Elliptic Curve Cryptography (ECC). The advantage of this proposed method is that the key can be distributed and managed without trusted centre, preserving the privacy of the key.A novel integrity auditing and re-signature method which verifies the data integrity. Whereas the downside is that Elliptical curve cryptography method is used which is complicated and also time consuming. Also use of asymmetric encryption technique in combination with symmetric encryption also increases the computation time

O. A. Khashan has used OutFS[4], a user-side encrypted file system, focused on providing a transparent encryption for stored and shared outsourced data. The benefit of this method is the key management is conveniently designed. The downside here is encrypting the file in user side leads to more access time for user which is not desirable.

H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang[5] have described an identity-based encryption transformation (IBET) model which seamlessly integrates two well-established encryption mechanisms, namely identity-based encryption (IBE) and identity-based broadcast encryption (IBBE).The advantage here is The user cannot see the encrypted data. They can only know the key and the decrypted version of the encrypted file. The disadvantage here is the use of identity based encryption leads to key escrow problem

O.A.Kashan [6]also provides hybrid proxy encryption scheme that combines symmetric and asymmetric for communications.The advantage of this system is this scheme can reduce the encryption and decryption overheads for end-users with resource-constrained devices. But the downside in this scheme is that these encryption techniques use asymmetric encryption which leads to significant computational complexity.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du and M. Guizani [7]have developed a reliable collaboration model consisting of three types of participants, which include data owners, miners, and third parties, where the data is shared via blockchain and recorded by a smart contract. The collaborative model used for storage of data is very reliable which is a great advantage. Disadvantage in this is data miner adds to the confidentiality issues

Shyla, S.I., Sujatha, S.S[8] have developed an efficient secure data retrieval is developed with the help of multi-stage authentication (MSA) and optimized blowfish algorithm (OBA) . The benefit of this development is after the encryption process, MSA based data retrieval process is performed. This will avoid, un-authorized person . But the disadvantage is that only one encryption algorithm is used which may make it easier for unauthorized person to decrypt the file if they get ahold of key.

M. Shah, M. Shaikh, V. Mishra and G. Tuscano[9] have proposed a system in which the user's file is encrypted and stored across multiple peers in the network using the IPFS (Inter Planetary File System) protocol. The advantage in this system is The decentralized storage method proposed in this paper is very strong and efficient. The disadvantage is that hash value of the addresses is stored which may lead to discovery of linked blocks using birthday attacks.

Jiaxing Li, Jigang Wu, Guiyuan Jiang, Thambipillai Srikanthan[10] have depicted the utilization of blockchain technique to develop a novel public auditing scheme for verifying data integrity in cloud storage. In the proposed scheme, different from the existing works that involve three participatory entities, data owner and cloud service. The upside of this method is Data owners store the lightweight verification tags on the blockchain. Using the hashtags reduces the overhead of computation and communication for integrity verification . Whereas the downside to this is use of third party auditors may lead to confidentiality issues

III. PROPOSED SYSTEM

An efficient cloud scheme with data in been made. Here we are using the erasure code technique for distribute the data to locations and access the data from. User can register and login into their account. Provided an option to store,share and access the data from storage. Here we are using the double ensured scheme for storing data into the cloud.

First is your data or file split into multiple parts and it will store into different server locations. Each and every file generates the key-code for auditing. Then second is each and every split file will encrypt before store into different locations. The shared users can edit the file in the with file owner’s permission. That file eligible of own public auditing. Search and download the files, at the time of download user should use the security key. As an authentication success it will be decrypt and combine to get the original data from. Moreover, we design a novel public verifiable authenticator, which is generated by a couple of keys and can be regenerated using partial keys.

Thus, our scheme can completely release data owners from online burden. In addition, we randomize the encode coefficients with a pseudorandom function to preserve data privacy. Extensive security analysis shows that our scheme is provable secure under random oracle model and experimental evaluation indicates that our scheme is highly efficient and can be feasibly integrated into the regenerating code- based storage.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

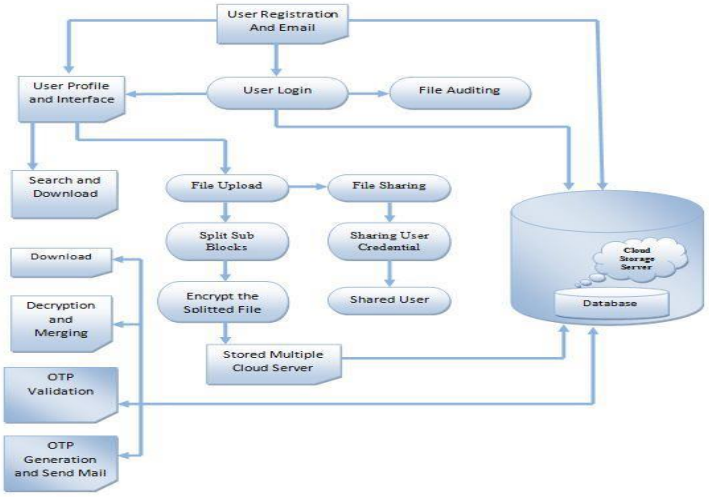

Figure 1: *System Architecture Diagram*

Figure 2: *Process Flow Diagram*

MODULE DESCRIPTION:

3.3.1 User Plug-In

In our Secure System we have a user friendly user interface to interact with our System. Every Act dual role as a data owner and data consumer while uploading file they are the owner of that file if they search other's file than they are the consumer. Users can create the account them self for that we have new pages, in that page we will get the details from the user and we generate the account for the user's. We have authentication system; we only allow authorized users to access our System.

In our System we providing the easy file searching user's don't want to keep remember all uploaded file's exact name, for that we have given the keywords while uploading the files it will help to search the file easily.

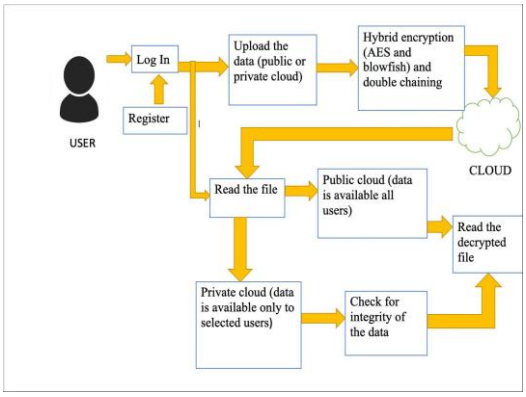

Figure 3: *Module Architecture*

3.3.2 Uploading File

Storing data over storage servers one way to provide data robustness is to replicate a message such that each storage server stores a message. Another way is to encode a message of k symbols into a codeword of n symbols by erasure

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

coding. To store a message, each of its codeword symbols is stored in a different storage server. A storage server corresponds to an erasure error of the codeword symbol. As long as the number of servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process.

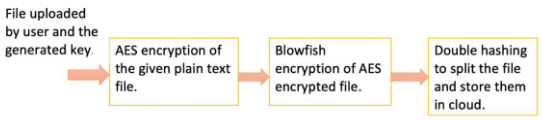

Figure 4: *Block diagram for file upload*

A. AES algorithm

The Advanced Encryption Standard (AES) algorithm is a symmetric block cipher that comprises three block ciphers,AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively.

Based on the key length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The continuous expansion in the number of internet and wireless communications users led to many security issues such as data privacy over the insecure networks to arise.

Thus, cryptography became one of the main approaches to secure and overcome attacks on the user's data. In November 2001, the National Institute of Technology and Standards (NIST) approved the AES cryptographic algorithm as the new encryption standard for its high security and flexibility. Ever since, many designs were introduced that were either aiming at high throughput as or at low memory consumption as. On the other hand, some were aiming at optimization between both parameters as and however, almost none were targeting to develop a design that consumes low power

B. Blowfish algorithm

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneir as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm.

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key expansion part and a data- encryption part. Key expansion converts a key of at the most 448 bits into several sub key arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent Permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. The Blowfish Encryption Algorithm contains 16 rounds; each round consists of XOR operation and a function (F).

Blowfish is fast, compact, simple and variably secure. Significantly faster than DES and optimized for application where key does not change like communication link or file encrypt or and not suitable for packet switching with frequent key changes or one-way hash function. A Feistel network is consisting of two parts – key expansion and data encryption. The key expansion converts a key of up to 448 bits into several sub key arrays totalling to 4,098 bytes. Data encryption consists of a simple function iterated 16 times. Each round consists of permutation and key. And, all operations are additions and XORs on 32bit words.

C. Double hashing

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneir as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm.

Blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key expansion part and a data- encryption part. Key expansion converts a key of at the most 448 bits into several sub key arrays totalling 4168

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent Permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. The Blowfish Encryption Algorithm contains 16 rounds; each round consists of XOR operation and a function (F).

Blowfish is fast, compact, simple and variably secure. Significantly faster than DES and optimized for application where key does not change like communication link or file encrypt or and not suitable for packet switching with frequent key changes or one-way hash function. A Feistel network is consisting of two parts – key expansion and data encryption. The key expansion converts a key of up to 448 bits into several sub key arrays totalling to 4,098 bytes. Data encryption consists of a simple function iterated 16 times. Each round consists of permutation and key. And, all operations are additions and XORs on 32bit words.

D. Checksum method

User can read all the files for which they have been given access. Once the user requests for a file, it is checked if it is in private cloud. If so, integrity constraint is checked using the checksum method. User is sent the key to their encrypted file using which the user decrypts the file. The decrypted can be downloaded by the user from the website and it is also sent to their mail. In checksum error detection scheme, the data is divided into k segments each of m bits. In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum. The checksum segment is sent along with the data segments. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented. If the result is zero, the received data is accepted; otherwise discarded**.**

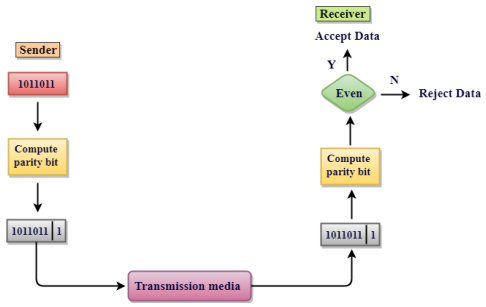

Figure 5: *Checksum process*

File Loading Process:

File downloading process is to get the corresponding secret key to the corresponding file to the user mail id and then decrypt the file data. The file downloading process re-encryption key to storage servers such that storage servers perform the re-encryption Operation .The length of forwarded message and the computation of re-encryption is taken

care of by storage servers. Proxy re-encryption Schemes significantly reduce the overhead of the data Forwarding function in a secure storage system.

Alert Mail

The uploading and downloading process of the user is first get the secret key in the corresponding user email id and then apply the secret key to encrypted data to send the server storage and decrypts it by using his secret key to download the corresponding data file in the server storage system's the secret key conversion using the Share Key Gen

IV. IMPLEMENTATION

The implementation work is carried out using PHP5
language using Code Ignitor in visual studio code editor
platform which enables us to program easily. The designing
of the proposed work is done using HTML 5, CSS. The database used here is MySQL. The cloud service used can be taken from the Amazon Web Services

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

V . RESULTS AND ANALYSIS

***Figure 6**: User registration*

Figure 7: User login

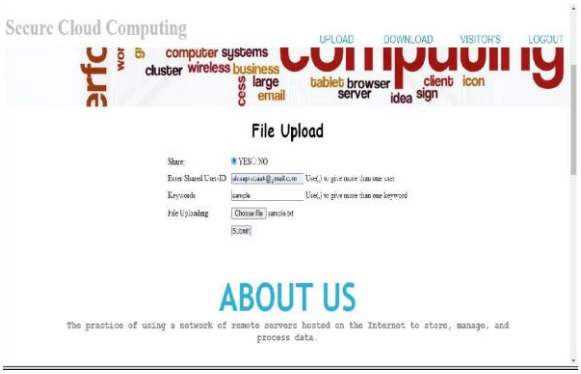

Figure 8: File upload

***Figure 9:** File download*

***Figure 10:** File updated*

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907190 |

Figure 11: *User approving the access of their file*

V. CONCLUSION

In conclusion , we have proposed system that promotes security as well as integrity of the data in cloud For security we use a novel threshold hybrid encryption scheme that the user data are encrypted by the Advanced Encryption Standard (AES), and the key seed of the AES is encrypted by the blow fish algorithm promoting the encryption efficiency and protecting data and key privacy, it makes the entire mechanism reliable and secure.

For integrity of data, multiple verification tasks from different users can be performed efficiently by the auditor and the cloud-stored data can be updated dynamically. It makes the clients check whether their outsourced data is kept intact without downloading the whole data. we are using the own auditing based on the token generation Anyone can download the files from the server with file owner permission. At the time of download key generated (code based key generation) and it will send to the file owner. We can download the file need to use the key for verification and some other users want to download file owner permission is necessary.

REFERENCES

[1] https://jelvix.com/blog/cloud-service-models.
[2] J. Li, H. Yan and Y. Zhang, "Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage," in *IEEE Transactions on Services Computing*, vol. 14, no. 1, pp. 71-81, 1 Jan.-Feb. 2021
[3] Shyla, S.I., Sujatha, S.S." Efficient secure data retrieval on cloud using multi-stage authentication and optimized blowfish algorithm",Link.springer.com (2021).
[4] Chen, Y., Liu, H., Wang, B*"* A threshold hybrid encryption method for integrity audit without trusted centre". Springeopen.com, *Vol* 10, no.3 (Jan 2021)
[5] O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in IEEE Access, vol. 8, pp. 210855-210867, Dec-2020.
[6] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, et al., "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud", *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3168-3180, 2020.
[7] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure Fog-to-Things environment", *IEEE Access*, vol. 8, pp. 66878-66887, 2020.
[8] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du and M. Guizani, "Blockchain-Based Incentives for Secure and Collaborative Data Sharing in Multiple Clouds," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1229-1241, June 2020, doi: 10.1109/JSAC.2020.2986619.
[9] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India,Vol 10, pp. 384-389,(2020).
[10] Jiaxing Li, Jigang Wu, Guiyuan Jiang, Thambipillai Srikanthan, "Blockchain-based public auditing for big data in cloud storage", Information Processing & Management, Volume 57, Issue 6, (2020)
[11] Zhang, Y., Yu, J., Hao, R., Wang, C., & Ren, K "Enabling Efficient User Revocation in Identity-based Cloud Storage Auditing for Shared Big Data" IEEE Transactions on Dependable and Secure Computing, vol 1, 2018

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details