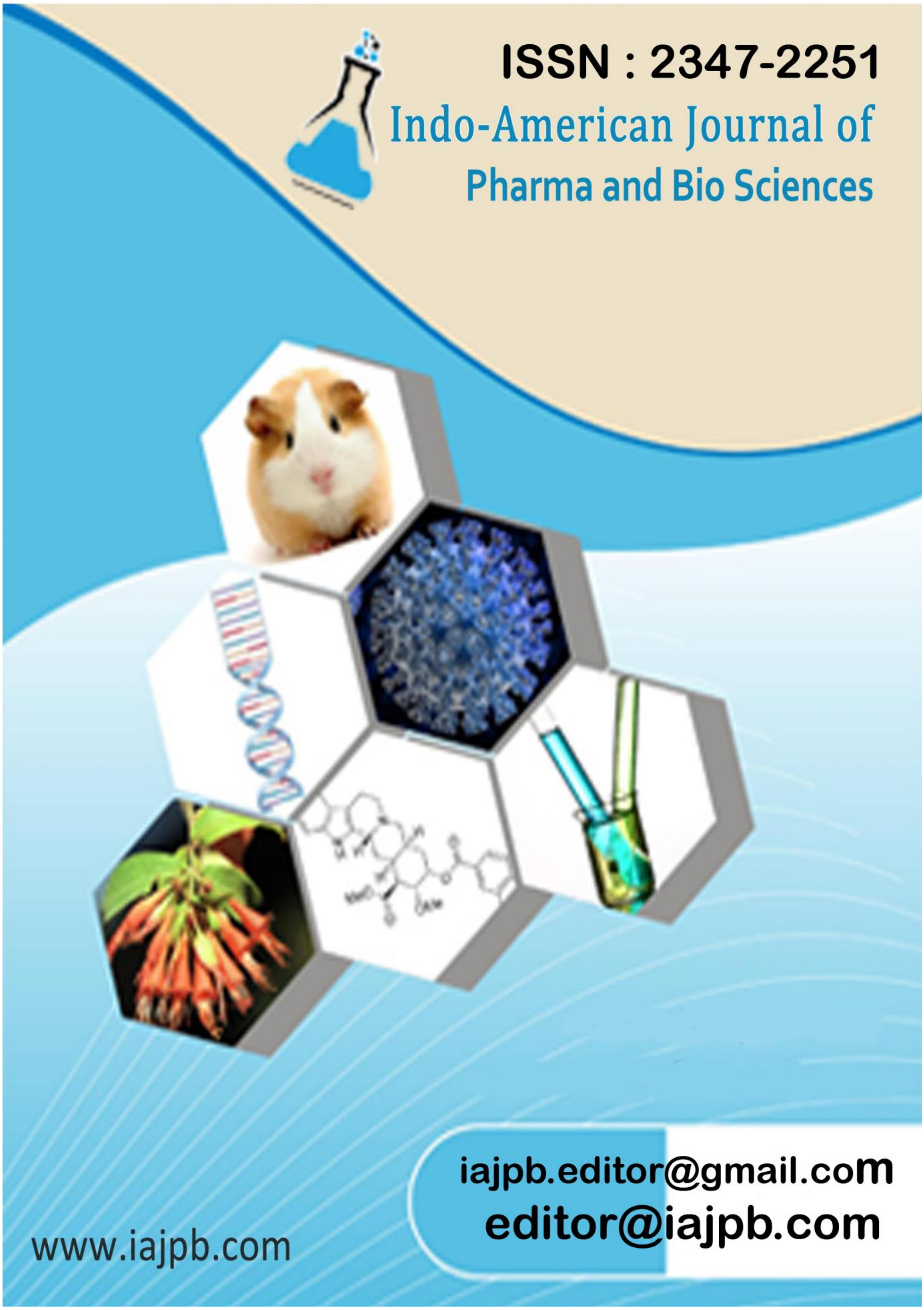


ISSN : 2347-2251

Indo-American Journal of Pharma and Bio Sciences

iajpb.editor@gmail.com
editor@iajpb.com

www.iajpb.com

Indo-American Journal of Pharma and Bio Sciences

Vol. 10, Issuse 3, July 2022

A DATA EXCHANGE PROTOCOL TO REDUCE CLOUD STORAGE DATAPROTECTIONRISKS INTHEBIG DATAERA

Linginedi Ushasree1,R.Madhuri Devi2

ABSTRACT: Using a cloud storage system, the data sharing service ensures that only trusted users have access to the information. In traditional systems, shared data is stored in data centers that are situated inside each party's own trust area. Cloud service providers, on the other hand, store this information in data centers that are not under the control of a single party, such as the data owner. This raises the question of data privacy. To keep sensitive data and communications safe from unauthorized access, this article outlines a secret key management mechanism for sharing groups (SSGK). For the first time in SSGK's history, it uses a secret sharing technique to share its encrypted group key. By using our protocol, we were able to save our customers 12 percent on storage space while still ensuring the privacy and security of their data.

Keywords:Secure data exchange in the cloud with SSGK, cloud service providers, and SSGK.

1.INTRODUCTION

This exciting future is being ushered in by today's cutting-edge big data technologies such as cloud computing and business intelligence, data mining, industrial information integration engineering, and the internet of things (IoT). Using the Internet as a distributed resource pool, cloud computing is a new paradigm for computing that distributes resources throughout the globe. Various applications and services may be given access to these resources on-the-fly. Companies may benefit from more adaptability, scalability, and efficiency in job execution by spending less money and using innovative task execution technologies. Enterprises will be able to more effectively use cloud computing services.their supercomputing and grid computing expendituresinsmartapplications.Notwithstandingthesebenefits,a major issue arises when personal data is kept on sucha cloud [7] [8]. There are compliance concerns withthis change since it would move sensitive data from afederationdomaintosomethinglikeadistributeddomain.Firstofallandforemost,beforeanyadvantage from big data technology can be obtained,the security and privacy issues raised in [9] and [10]shouldbedealt with.

1PGScholar,Dept.ofCSE,PriyadarshiniInstituteofTechnologyandManagement,Guntur,AP,India
2AssociateProfessor,Dept.ofCSE,PriyadarshiniInstituteofTechnologyandManagement,Guntur,AP,India.Ushalinginedi1413@gmail.com1,madhuridevichandu@gmail.com2

Developingacloudstoragesecurity systemisverydifficult.Awaytoaddresstheproblemofsharedinformation in the cloud would be to allow it to beaccessed by legitimate users in some kind of a timelymanner. And in a similar way, growing numbers oforganisations, devices, and apps using the cloud makesitevenharderto maintaingoodaccesscontrol, since

A higher number of points of entry are available for attack. Sharing data in the cloud is vulnerable to being lost or purposely damaged by the cloud provider and network hackers. One of the most difficult tasks is to ensure that shared data cannot be deleted, updated, or tampered with.

To protect a shared system, there have been two conflicting methods in the past. Network access [11] is a technique that restricts access to shared data to users registered in the access control table. The use of a group key [12]_[16] to safeguard shared data is another option. Users can't get their hands on data that doesn't belong to them even if an access control mechanism is in place. Traditionally, a third party is needed to hold the group key under their control in conventional large systems. Using these methods necessitates the belief that the third party has always been trustworthy. However, in the case of cloud storage, this assumption is incorrect.

Secret sharing group key management system is introduced in this article to help with cloud storage information sharing. This protocol takes numerous precautions to prevent or detect fraud. The first step is to identify the problem.toprotecttheshareddatausingsymmetricencryption

[17] techniques to make it useable by authorised userswhen they need it. Once someone decides to share data,the owner distributes the encryption keys to everyonethat's allowed to access it. Second, whomever has thedecryptionkeycontrolsallpermissionsformaterialthat's been shared. Cryptographic techniques [18] thatutilise asymmetric encryption are employed to encryptthe interactive communication, meaning only permittedparticipants have had the capability to decode the key.The protocol utilises secret sharing can assign a keyamonglegitimateparticipantsinsidetheeventthatshared material is discovered by unauthorised parties.Wegetasecurity-awarecloudbyensuringtheprotection of information shared inside this cloud. Withsecurity mechanisms built into the cloud storage, anyclouddeploymentcouldproceedrapidlyinsuchamission-criticalbusiness situation.

LITERATURESURVEY

1. "Efficient and secure identity-based encryptionschemewithequalitytestincloudcomputing,"XinyiHuanget.al[1](2015)Introducingaringsignature Identity-based (ID-based) that removes thecertificate verification procedure. The safety level ofthe ring signature was improved by offering a secureID-basedcirclesignaturetechnique.Thistechniqueincludes previously produced signatures of that if anuser's secret key was compromised and the accountremains valid. When a single patient's secret key wascompromised,subsequentdataownerscan notre-
2. provide evidence of the accuracy of each piece of information. Because it is so effective and doesn't need any combination methods, it is an absolute necessity for any large-scale data sharing system. User secret keys are merely integers, while updating the key requires an exponentiation. There are certain drawbacks to this system, including the need for user identification and privacy.
3. "Attribute set based access control with both sharing and full delegation of privileges in cloud computing" Research by Huang Qinlong et al (2015) Recommendation of an attribute-based secure cloud computing technique for Efficient Revocation (EABDS). Symmetrical encryption is used to encrypt data, and then Ciphertext policy attribute-based encryption is used to encode the encrypting data (CP-ABE). The homomorphic encryption approach may be used to solve the

problem of key escrow by creating solely for key attributes supported by the attribute authority of a key server. By only generating the secret key attributes, this homomorphic encryption approach prohibits data from being accessed by attribute authorities. The EABDS system promptly revokes the qualities, providing both forward and backward security, as well as assuringreducing user calculations costs. The benefits of thistechniquearecleanerandmoreeffective.

4."Securing outsourced data in the multi-authoritycloud with fine-grained access control and efficientattributerevocation,"HongLiuet.al[3](2015)proposed a privacy declaration based on the SAPA (Shared Authority-based Authentication Protocol) to address issues with cloud storage privacy. Using its protocol, it's possible to run many cloud apps simultaneously. Authentication is the mainstay of contemporary security measures. SAPA uses an anonymous requester matching approach to perform shared access permission, provides Ciphertext attribute-based access control so that users may reliably access their own data fields, and the proxy re-encryption is employed to enable data sharing across numerous users.. The SAPA's design correctness is shown by the development of the universal composite capability (UC) model. If a client is having trouble with a cloud server, they may have to ask other users to exchange information, which might reveal the user's personal information. Patients' sensitive privacy is protected by this system, which provides access control, login authority sharing, and privacy preservation when the patient is online. The SAPA protocol ensures authentication and authorization while safeguarding confidential customer information.

5.Privacy-preserving public auditing for securecloud storage," Xin dong et.al [4] (2014), Proposedanefficient,scalableandadaptable,semanticsecurity datapolicy.TheyutilisedtwoCiphertex(CP-ABE)& 6. Individual Identity Encryption (IBE) approaches, a secure, cloud-based data sharing solution that allows dynamic data access. Strong data sharing ensures the privacy of cloud users and allows for dynamic operations such as file production, user revocation or user-entered alterations to be carried out quickly and securely. It also enforces sophisticated access control, total resistance to collusion, and reverse secrecy via the use of this technology. Cloud computing may be more affordable for people and businesses, but it does not guarantee their privacy or security. The generic Bilinear group model with access confidentiality and secrecy is used to provide semantic security in cloud computing information sharing. Compared to present systems, such a system's overall performance analysis has a low overhead.

7. "SecureMulti-AuthorityDataAccessControl Scheme in Cloud Storage SystemBasedonAttribute-basedSignencryption"QiangTanget.al[5](2014) A searchable encryption system for multi-party data is recommended (MPSE). Selective decryption enables the user to view their encrypted data at their own pace. There is still another model of security offered for the worst-case and typical scenarios

individual consumer dynamics result in a scenario collusion. The new approach he proposed was well-tested and confirmed to be secure. An MPSE security approach, on the other hand, provides more peace of mind. In the MPSE formulation, only at the index level can Alice determine whether or not Bob may search for, which implies that when all keywords seek to utilize allowed keywords, Alice can decide whether or not Bob can search for. On the indexes of Bob, Alice has allowed the search for only a few keywords and Bob's colluding cloud server may get the term for all Alice searches. All indexes Alice has authorized are meant to have a single trapdoor search problem, according to this MPSE phrasing. Among this formula's flaws are Using several key index pairs with various peers exposes Alice to more unnecessary information. The row-column structure, on the other hand, is unable to deal with this sort of problem.

IMPLEMENTATION

ExistingSystem

Personal health records may be securely shared in the cloud using ciphertextpolicy-attributed-based (CP-ABE) signcryption, according to Rao. It focuses on controlling access to private data by unauthorized parties.

For personal records in cloud computing, Liu et al. developed an access control strategy based on CP-ABE.

⍰Huangetal.introducedanovelpublickey encryption withauthorized equalitywarrantsonallofitsciphertextoraspecifiedciphertext

Disadvantages

It'simportanttorememberthatthereisreallyisnogroup-basedadmissioncontrol mechanism in the project we arefinishing.

Anyone who has a copy of the t shares may participate. The secret sharing concept was improved by Chor et al. [32], who made it verifiable (VSS). Shareholders have the option of verifying the accuracy of their investments.

Advantages

Sobecausedataowneriscompletelytrustworthy and incorruptible, the data will not becompromised.

Owing to a lack of robust encryptionmethods,thesystem'ssecurityisextremelylow.

ProposedSystem

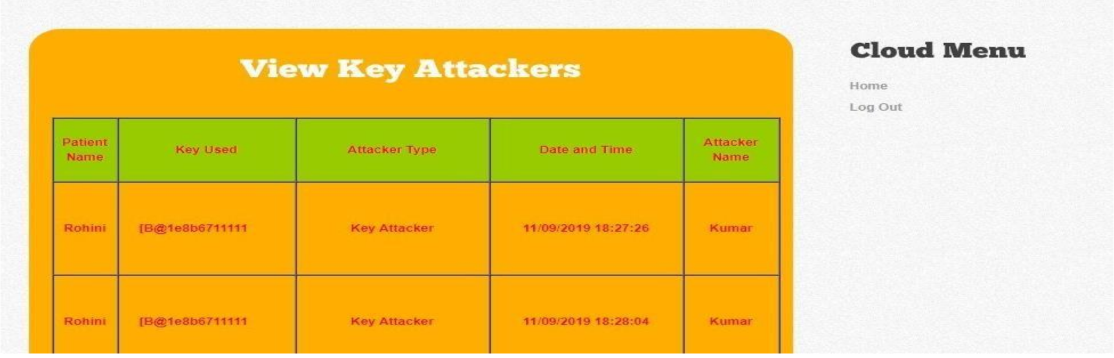
The efficient solution provided in SSGK may improve the security of the information given here on cloud storage without the need for a third party. Asymmetric algorithm and secret sharing scheme were employed to make it more difficult for unauthorized users to get the keys needed to decode the shared data. In order to safeguard cryptographic keys, Blakley [30] and Shamir [31] developed secret sharing systems in 1979. The persons who have access to a secret are protected by secret sharing methods that divide the information into smaller bits for those who have been entrusted with it. It is possible to reassemble the pieces of this puzzle.Because of the group key that is given forth viathesecretsharingmethod,thesystemismuch more secured Every members of the team may findand collect various sub-secret shares in order tobuild agroupkey.

ResultsandDiscussion

Figure.2 depicts a distributed storage information sharing paradigm for several components. There are three types of components in the convention model: a cloud service provider, a data owner, and attendees. The provider of the cloud: offers information owners a public stage on which to store and distribute their encoded data. Owners have complete control on who has access to their data, not the cloud provider. Any client may publicly download the encoded data. The proposed SSGK's information convention paradigm. Proprietor of information: describes the approach and uses a gathering key to encrypt its data via a symmetric encryption computation. Individuals that successfully completed the admission approach form a sharing group. A secret sharing plan is used to distribute the encryption key to the sharing community at that moment. Each member of the group, including the information owner, is given a book and a few keys. The public cloud is open to everyone, so anyone can access whatever interesting encrypted data they're interested in. However, if and only if the information owner gives the decoding key to the client, the information may be decoded. In SSGK, we have the following presupposition: The owner of the information can be relied on to keep it safe from the hands of any adversaries. In spite of the fact that the cloud service provider is semi-trusted, they would nevertheless try to find as much mysterious data as possible based on the information that the data owners have transmitted to them for financial gain. SSGK's security concept is now shown via the publishing of prospective attacks. The commotion

By conducting the mystery sharing conspiracy, the key is spread. The collecting key may be reproduced by assembling the subsecret offers of various members of the group. Every pair of members has a highlight point channel to transmit messages, which further describes our convention's communication system.

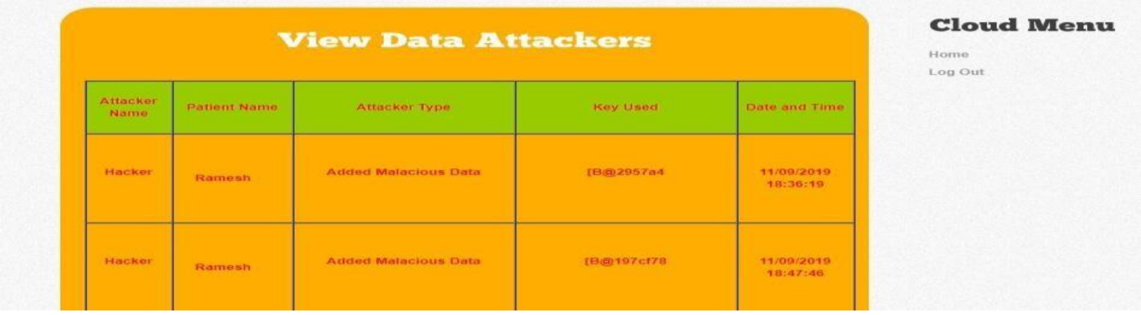
EXPERIMENTALRESULTS:



Patient Name	Key Used	Attacker Type	Date and Time	Attacker Name
Rohini	[B@1e8b6711111	Key Attacker	11/09/2019 18:27:26	Kumar
Rohini	[B@1e8b6711111	Key Attacker	11/09/2019 18:28:04	Kumar

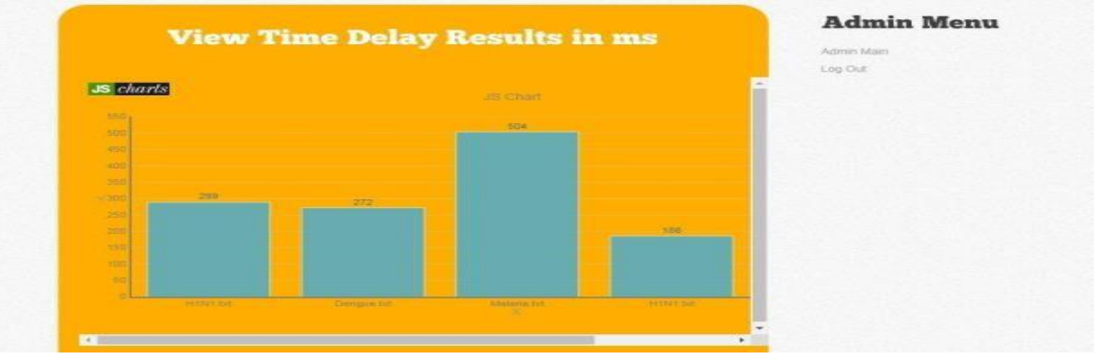
Fig:ViewKeyAttackers

Fig:ViewDataAttackers



Attacker Name	Patient Name	Attacker Type	Key Used	Date and Time
Hacker	Ramesh	Added Malacious Data	[B@2957a4	11/09/2019 18:36:19
Hacker	Ramesh	Added Malacious Data	[B@197cf78	11/09/2019 18:47:46

:



VFig:ViewDataThroughputinchart

Fig:ViewTimeDelayResults

CONCLUSIONS

We provide a novel protocol for group key management that makes it possible to share cloud data. By using RSA and verified private keys, the data owner may have complete control over external information without having to rely on anybody else. GKMP's robustness is shown through a detailed examination of possible threats and effective solutions. The data storage and computational complexity of our protocol have also been decreased by our method. Grid-private data in cloud storage is protected using this scheme's security technique. The grid data can only be accessed by authorized parties thanks to cryptography and an approved security mechanism. Our technique becomes more viable with better data and computer power.

The protocol for group key management may need to be tweaked to address the problem of forward and reverse security. The group members technique, which is both efficient and scalable, is still the future of work.

REFERENCES

On lowering energy costs in Internet-scale systems with dynamic data [1]: P. Zhao (with W. Yu), S. Yang (with S. Yang), X. Yang (with J. Lin), IEEE Access, vol. 5, pp. 20068_20082, 2017.

A fuzzy preference tree-based recommender system for customised business-to-business E-services by D. Wu, G. Zhang, and J. Lu was published in IEEE Transactions on Fuzzy Systems in February 2015, volume 23, number 1.

In the paper by X. Wu, X. Zhu, GQ. Wu, and W. Ding titled "Data mining using huge data," IET Knowledge and Data Engineering, 26, 97-107 Jan. 2014.

X. Shi, L. X. Li, L. Yang, Z. Li, and J. Y. Choi

Industrial information integration: a study of reverse logistics information flow Information and Technology Management, Volume 13, No. 4, pp. 217_232, December 2012.

"SDN and virtualization options for the Internet of Things: A survey," IEEE Access, vol. 4, no. 5, may 2016, pp. 5591 5606.

All of the above-mentioned researchers contributed to this study.

Inte- prise Inf. Syst., vol. 6, no. 2, pages 165_187, November 2012, "Integration of hybrid wireless networks with cloud services-oriented enterprise information systems,"

S. A. Thekdi and K.-Y Teng, J. H. Lambert,

‘‘Assessment of risk and safety program effectiveness and modeling of business processes" Vol. 42, No. 6, pp. 1504 1513 in IEEE Transactions on Systems, Man, and Cybernetics A, Sys. Humans

[8] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search across encrypted outsourced data in cloud," in Proc. 35th Annu. IEEE Int. Conf. Commun.

[1] J.Han,W.Susio,Y.Mu,andJ.Hou, ``Improvingprivacyandsecurityindecentralized ciphertext-policyattribute-basedencryption,''IEEETrans.Inf.ForensicsSecurity,vol.10,no.3,pp.665_678, Mar. 2015.

[2] D.Zou,Y.Xiang,andG.Min, ``Privacypreservingincloudcomputingenvironment,'' Secur. Commun. Netw., vol.9,no. 15, pp. 2752_2753 Oct. 2016.

[3] Y. Tang, P. P. C. Lee, John C. S. Lui,andR.Perlman,``Secureoverlaycloudstoragewithaccesscontrolandassureddeletion,'' IEEE Trans. Dependable SecureComput.,vol.9,no.6,pp.903_916,Nov./Dec.2012.

[4] J. Shao, R. Lu, and X. Lin, ``Fine-graineddatasharingincloudcomputingfor mobile devices,'' in Proc. IEEE Conf.Comput.Commun.(INFOCOM),Apr./May 2015, pp. 2677_2685.

[5] C.Wang,S.S.M.Chow,Q.Wang,
K. Ren, and W. Lou, ``Privacy preservingpublicauditingforsecurecloudstorage,''IEEETrans.Comput.,vol.62,no.2,pp.362_375 ,Feb. 2013.

[6] S.Tanada,H.Suzuki,K.Naito,and
A. Watanable, ``Proposal for secure groupcommunicationusingencryptiontechnology,'' in Proc. 9th Int. Conf. MobileComput. Ubiquitous Netw., Oct. 2016, pp.1_6.

[7] J. Zhou et al., ``Securing outsourceddata in the multi-authority cloud with _ne-grainedaccesscontrolandef_cientattribute

revocation,'' Comput. J., vol. 60,no.8, pp. 1210_1222, Aug. 2017.

[8] R.Ahuja,S.K.Mohanty,andK.Sakurai,``A scalableattribute-set-basedaccesscontrolwithbothsharingandfull-_edgeddelegationofaccessprivilegesincloudcomputing,''Comput.Elect.Eng.,vol.57,pp.241_256,Jan. 2017

[9] J. Thakur and N. Kumar, ``AES and blow_sh:Symmetrickeycryptographyalgorithmssimulationbasedperformanceanalysis,''Int.J.Emerg. Technol. Adv. Eng., vol. 1, no. 2, pp. 6_12,Dec.2011.

[10] E. Fujisaki, T. Okamoto, ``Secure integrationofasymmetricandsymmetricencryptionschemes,'' J. Cryptol., vol. 26, no. 1, pp. 80_101,Jan.2013.

[11] Y. S. Rao, ``A secure and ef_cient ciphertext-policyattribute-based signcryption forpersonalhealthrecordssharingincloudcomputing,'' Future Gener. Comput. Syst., vol. 67,pp.133_151 Feb. 2017.

[12] S. Jin-Shu, C. Dan, W. Xiao-Feng, and S. Yi-Pin,``Attributed-basedencryptionschemes,''J.Softw.,vol. 22, no. 6, pp. 1299_1315, 2011.

[13] H.liu,Y.huang,andJ.K.Liu,``Securesharing ofPersonalHealthRecordsincloudcomputing: Ciphertext-PolicyAttribute-BasedSigncryption,'' Future Gener. Comput. Syst., vol.52,pp. 67_76, Nov. 2015.

[14] K.Huangetal.,``PKE-AET:Publickeyencryption with authorized equality test,'' Comput.J.,vol. 58, no. 10, pp. 2686_2697, Oct. 2015.

[15] L.Wu,Y.Zhang,K.-K.R.Choo,andD.He, ``Ef_cientand secureidentitybased encryptionschemewithequalitytestincloudcomputing,'' Future Gener. Comput. Syst., vol. 73,pp.22_31, Aug. 2017.