A comparative study on different data aggregation approaches in cloud IoT

Harikrishnan K, Gowrimanohari K

DOI: 10.29322/IJSRP.11.11.2021.p11965
http://dx.doi.org/10.29322/IJSRP.11.11.2021.p11965

Abstract- Cloudi iremovesi iassociationsi ifromi ibuildingi iupi iin-housei iinformationi istockpilingi iframeworks.i iNonetheless,i idistributedi istoragei ileadsi itoi isecurityi iconcerns.i iCloud-expliciti iandi itraditionali iinsideri idangersi iarei ilookedi ibyi iinformationi iifi itherei ishouldi iarisei iani ioccurrencei iofi igatheringi isharedi iinformation.i iThei isignificanti iissuei iisi ithei iSecurei idatai isharingi ibetweeni iai igatheringi ithati icountersi iinsideri idangersi iofi iauthentici iyeti iperniciousi iclients.i iIni ithisi ipaper,i iwei iproposei ithei iSecurei iDatai iSharingi iini iCloudsi iprocedurei ithati igives:i i1)i iinformationi iprivacyi iandi itrustworthiness;i i2)i iaccessi icontrol;i i3)i iinformationi isharingi i(sending)i iwithouti iutilizingi iregisteri iseriousi ire-encryption;i i4)i iinsideri idangeri isecurity;i iandi i5)i iforwardi iandi iini ireversei iaccessi icontroli i6)i iOnei itimei idownloadi i7)i iSharei iTimei iExpirei i8)i iSecreti iKeyi iManagement.i iThei iSecurei iinformationi isharingi isystemi iencodesi iai irecordi iwithi iai isolitaryi iencryptioni ikey.i iThei iclienti igetsi ijusti ionei idividei ibetweeni ithei itwoi idistinctivei ikeyi ioffersi ithati iarei icreatedi ifori ieveryi iclient.i iThei iownershipi iofi iai isolitaryi iportioni iofi iai ikeyi ipermitsi ithei iSecurei iinformationi isharingi iprocedurei itoi icounteri ithei iinsideri idangers.i iThei iotheri ikeyi iofferi iisi iputi iawayi ibyi iai iconfidedi iini ioutsider,i iwhichi iisi iknowni iasi ithei icryptographici iworker.i iThei iSecurei iinformationi isharingi istrategyi iisi irelevanti itoi icustomaryi iandi iversatilei idistributedi icomputingi iconditions.i iWei icarryi iouti iai ifunctioningi imodeli iofi ithei iSecurei idatai isharingi iapproachi iandi iassessi iitsi ipresentationi independenti ioni ithei itimei idevouredi iduringi idifferenti iactivities.i iThei ioutcomesi iendi iupi ibeingi iempoweringi iandi ishowi ithati iSecurei iinformationi isharingi icani ipossiblyi ibei iadequatelyi iutilizedi ifori isecurei iinformationi ipartakingi iini ithei icloud.

Index Terms- iSecurei idatai isharing,i iTriplei iDES,i iBlowfishi i,i ireencryption,i iKey,i icloud.

I. Introduction

Distributedi icomputingi ijoiningi iai ibunchi iofi iexistingi iandi inewi iproceduresi ifromi iresearchi iregions,i ifori iexample,i iadministrationi iarrangedi imodelsi i(SOA)i iandi ivirtualizationi iisi iconsideredi iasi ithei ifollowingi istagei iini ithei idevelopmenti iofi ion-requesti idatai iinnovation.i iIti iisi istandardi ifori iclientsi itoi iusei idistributedi istoragei iadministrationsi itoi iimparti iinformationi itoi iothersi iini iai icompanioni icircle,i ie.g.,i iDropbox,i iGooglei iDrivei iandi iAlii iCloud.i iThei icommoni iinformationi iini icloudi iworkers,i inonetheless,i itypicallyi icontainsi iclients'i itouchyi idatai i(e.g.,i iindividuali iprofile,i imonetaryi iinformation,i iwellbeingi irecords,i iandi isoi ion)i iandi ishouldi ibei iveryi imuchi isecured.i iAsi ithei iresponsibilityi ifori iinformationi iisi iisolatedi ifromi ithei iorganizationi iofi ithem,i ithei icloudi iworkersi imayi irelocatei iclients'i iinformationi itoi iotheri icloudi iworkersi iini ireevaluatingi iori iofferi ithemi iini icloudi ilooking.i iIni ithisi imanner,i ithei ilargei itesti iisi itoi iensurei ithei iprotectioni iofi ithosei icommoni iinformationi iini icloud,i iparticularlyi iini icross-cloudi iandi ienormousi iinformationi iclimate.i iThisi itesti icani ibei imeti ibyi iplanningi iai icompletei iansweri ifori ihelpi iclienti icharacterizedi iapprovali iperiodi iandi itoi igivei ifine-grainedi iadmittancei icontroli iduringi ithisi iperiod.i iAfteri ithei iclienti icharacterizedi iterminationi itimei ithei icommoni iinformationi ioughti itoi iacti inaturallyi iannihilated.i iThei iinformationi iisi iputi iawayi iini iai itypicali iencodedi istructurei itoi ilighteni ithei iissues.i iThei iclienti ican'ti isharei ihis/heri iencodedi iinformationi iati iai ifine-grainedi ileveli iwhichi iisi iai ihindrancei iofi iscramblingi iinformation.i iThei iproprietori ishouldi iknowi idefinitei isubtletiesi iofi ithei ionei ihe/shei ineedsi itoi iimparti ito.i iIni inumerousi iapplications,i ithei iinformationi iproprietori ineedsi itoi iimparti idatai itoi iai ifewi iclientsi iasi iindicatedi ibyi ithei isecurityi istrategyi independenti ioni ithei iclients'i iqualifications.i iThei icriticali ibenefitsi iofi iAttributei ibasedi iencryptioni i(ABE)i iisi ithati iiti idependsi ioni ithei icustomi ipublici ikeyi iencryptioni iratheri ithani ibalancedi iencryptioni isincei iiti iaccomplishesi iadaptablei ione-to-numerousi iencryption.i iToi iaccomplishi ibothi ihighi iinformationi isecurityi iandi ifine-grainedi iadmittancei icontrol,i ithei iincrediblei istrategyi iisi igiveni ibyi iTriplei iDESi iplani iandi iblowi ifishi iencryptioni icalculationi iTriplei iDatai iEncryptioni iStandardi i(DES)i iisi iai ikindi iofi iautomatedi icryptographyi iwherei isquarei icodei icalculationsi iarei iappliedi imultiplei itimesi itoi ieveryi iinformationi iblock.i iThei ikeyi isizei iisi iexpandedi iini iTriplei iDESi itoi iguaranteei iextrai isecurityi ithroughi iencryptioni icapacities.i iEachi isquarei icontainsi i64i ipiecesi iofi iinformation.i iThreei ikeysi iarei ialludedi itoi iasi ipacki ikeysi iwithi i56i ipiecesi ifori ieachi ikey.i iBlowfishi iisi iai isymmetrici iencryptioni icalculation,i iimplyingi ithati iiti iutilizesi iai isimilari imysteryi ikeyi itoi ibothi iencodei iandi idecodei imessages.i iBlowfishi iisi iadditionallyi iai isquarei icode,i iimplyingi ithati iiti isplitsi iai imessagei iintoi ifixedi ilengthi iblocksi iduringi iencryptioni iandi iunscrambling.i iThei isquarei ilengthi ifori iBlowfishi iisi i64i ipieces;i imessagesi ithati iarei icertifiablyi inoti iai idifferenti iofi ieighti ibytesi iini isizei ishouldi ibei icushioned.i iAccordinglyi iini ithisi ipaperi ithei iinformationi iisi isharedi isafelyi iini icloudi ithroughi

iencryptioni icalculationi iandi ithei iinformationi iisi isharedi itoi ianotheri iclienti iwithi ithei iassistancei iofi imysteryi ikeyi iapproval.

II. LIITERATURE SURVEY

On the works of Akhil K M et al., a scheme was proposed that focused on ensuring the protection of data transfers through the use of encryption techniques. The problem with the third-party auditor was taken into account by the procedure. The third party was refused access to the user data in this scheme. The results showed that the proposed approach improved the system's overall security by making it more difficult for intruders to break the data being transferred.[1]

Akhil, K. M., Kumar, M. P., & Pushpa, B. R. (2017, June). Enhanced cloud data security using AES algorithm. In *2017 International Conference on Intelligent Computing and Control (I2C2)* (pp. 1-5). IEEE.

The works of Jun Zhon et al., aided in the creation of a modern architecture as well as specific security and privacy standards for next-generation mobile applications on cloud-based IoT. Without using public key homomorphic encryption, the new approach helped to preserve user authentication. Finally, a number of intriguing open problems are proposed, along with exciting ideas for further research in this developing field. [2]

Zhon, J. (2017). Security and privacy for cloud-based IoT: Challenges, countermeasures, and future directions. *IEEE Communication Magazine*, *55*(1), 26-33.

The research of Debiao He et al., in the smart grid setting, proposed a light-weight data aggregation scheme using (ECC). The proposed system's main aim was to reduce computing costs while improving security. The method can provide confidentiality, authenticity, and credibility, according to security research. The cost of computation and communication is significantly lower than in previous systems, according to performance analysis. As a result, it can be inferred that this scheme is more realistic for smart grid implementation [3].

He, D., Zeadally, S., Wang, H., & Liu, Q. (2017). Lightweight data aggregation scheme against internal attackers in smart grid using elliptic curve cryptography. *Wireless Communications and Mobile Computing*, *2017*

The research works of Sunantha Nalajal et al., helped in proposing the framework which is robust three-factor authentication with the aid of password, biometrics and mobile device which provides secure security strength to the user's data and allows counter attack to existing attack. This scheme not only encountered security problems but also provided with most enhanced security functionalities [4].

Nalajala, S., Moukthika, B., Kaivalya, M., Samyuktha, K., & Pratap, N. L. (2020). Data Security in Cloud Computing Using Three-Factor Authentication. In *International Conference on Communication, Computing and Electronics Systems* (pp. 343-354). Springer, Singapore.

Sandeep K. Sood et al., proposed a system that consists of various techniques and advanced procedures that can effectively secure data from start to finish. Data is classified according to its level of confidentiality, integrity, and availability. For protection, the strategy employs measures such as Secure Socket Layer and Message Authentication Code. It also adds more complexity and versatility to meet the needs of today's dynamic and diverse network [5].

Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. *Journal of Network and Computer Applications*, *35*(6), 1831-1838.

The research of M.Shobhana et al., aided in the development of an effective model for data confidentiality, integrity, analysis, and false data detection in order to make the network more safe during data forwarding and aggregation. The computational overhead and network complexities are significantly minimised, according to the results. Future work can be improved in real-time implementations, as well as greater privacy while maintaining security. [6]

Shobana, M., Sabitha, R., & Karthik, S. (2020). An enhanced soft computing-based formulation for secure data aggregation and efficient data processing in large-scale wireless sensor network. *Soft Computing*, 1-12.

The works of D. Vinodha et al., examined the various data aggregating options that are currently available. The authors make an attempt to categorise them based on the node architecture and privacy methods used. The systems are compared based on privacy factors such as confidentiality, integrity, and authentication, which reveals how well they support scalability, multiplication, and data recovery [7].

Vinodha, D., & Anita, E. M. (2019). Secure data aggregation techniques for wireless sensor networks: a review. *Archives of Computational Methods in Engineering*, *26*(4), 1007-1027.

The research conducted by Chandu Y et al., suggested a methodology that allows the edge device to encrypt data using the Advanced Encryption Standard (AES) before sending it to the cloud. The RSA crypto system is used to encrypt the AES key. For various conditions, the results have been demonstrated to be stable, secure, and attack proof [8].

Chandu, Y., Kumar, K. R., Prabhukhanolkar, N. V., Anish, A. N., & Rawal, S. (2017, August). Design and implementation of hybrid encryption for security of IOT data. In *2017 International conference on smart technologies for smart nation (SmartTechCon)* (pp. 1228-1231). IEEE.

Mahmoud Ammar et al., analysed the security of the main IoT frameworks, which totalled eight. The proposed architecture, the essentials of developing third-party smart apps, appropriate hardware, and security aspects were all clarified for each frame work. When comparing the standards used to secure communications, it was discovered that different approaches were employed to provide other security features [9].

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27.

The works of Feyza Yildirim Okay et al., introduced, a unique Domingo-Ferrer additive privacy based Secure Data Aggregation (SDA) approach for fog computing-based smart grids. When compared to existing methods, the suggested protocol had a faster response time and a lower computing overhead. In terms of data transmission and storage efficiency, there was also a big improvement. Furthermore, a security study revealed that the

suggested technique successfully protects the privacy of the data acquired. [10]

Okay, F. Y., & Ozdemir, S. (2018, April). A secure data aggregation protocol for fog computing based smart grids. In *2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018)* (pp. 1-6). IEEE.T

The works of Devi P et al., proposed that in light of homomorphic encryption conspired for security protection, offered a system where the primary focus is on open key cryptography algorithm. The investigation focuses on several homomorphic encryption standards and features. It gives useful data on several aspects of service quality, such as exhibition time, key generation time, and efficiency comparison.[11]

Devi, P., & Sathyalakshmi, S. (2020). A Comparative Study on Homomorphic Encryption Algorithms for Data Security in Cloud Environment. *environment, International*, *11*(2), 129-138.

The works of Qinglei Kong et al., aided in the development of a scheme that protects data content using the homomorphic Pallier cryptosystem and the truncated alpha geometric approach. On a time series sliding window basis, this scheme also aggregated and authenticated collected data. When compared to the previous way, this strategy offers significant improvements in communication and processing overhead.[12]

Kong, Q., Lu, R., Yin, F., & Cui, S. (2020). Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud. *IEEE transactions on Intelligent Transportation Systems*.

The research done by Cheng Guo et al., offered a methodology that indicates that the proposed approach has secured plain text assault resilience assault under the computational Diffe-Helman assumption. The difficulty of the assumption is used to evaluate the scheme. According to a comparative research, this methodology allows for privacy-protected medical data aggregation.[13]

Guo, C., Tian, P., & Choo, K. K. R. (2020). Enabling privacy-assured fog-based data aggregation in e-healthcare systems. *IEEE Transactions on Industrial Informatics*, *17*(3), 1948-1957.

The research done by Saket Komawar et al., offered a way for executing privacy-preserving transitions on a secured cloud without decrypting the data This system protects users who exchange data for analysis because the private keys do not need to be shared with the researcher, who can conduct analysis on the cypher text without having access to the plain text. Other dynamic processes, such as multiplication, may be added to the proposed work with differential privacy.[14]

.Komawar, S., Batwal, M., Shah, S., Shahani, S., & Abraham, J. (2018, August). Privacy Preserving Data Aggregation on Secure Cloud. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1-5). IEEE.

The proposed method by Ismile Butun et al., assisted in the development of an IDS algorithm, as well as a survey on fog computing's integration with IoT and its consequences. The project's purpose was to uncover and highlight concerns that arise when fog computing is employed by IoT, notably security-related issues. Despite the fact that this integration looks to be tough and time-consuming, the results show that it has no benefits other than security implications. [15]

Butun, I., Sari, A., & Österberg, P. (2019, January). Security implications of fog computing on the internet of things. In *2019 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-6). IEEE

The work of David Sanchez et al., semantically grounded data splitting system was developed that can automatically identify and break data chunks that potentially cause privacy risks on local premises, ensuring that each chunk is risk-free. Because requests were processed in a transparent manner on cloud premises, outsourced functionality was simply enabled by broadcasting requests to several cloud locations. [16]

Sánchez, D., & Batet, M. (2017). Privacy-preserving data outsourcing in the cloud via semantic data splitting. *Computer Communications*, *110*, 187-201

The research of Firas Al Doghman et al., aided in the overview of various data aggregation methodologies in IoT infrastructure a novel type of data aggregation algorithm is also discussed. This innovative technique uses a consensus-based aggregation with fault tolerances methodology in fog computing. This novel strategy stimulates adaptive behaviour and enables for more efficient aggregate result distribution to ascending nodes. [17]

Al-Doghman, F. Q. M. S. (2019). Consensus-Based Data Management within Fog Computing For the Internet of Things (Doctoral dissertation).

The work of Prathiba Mudra et al., proposed a system in which the methodology explored data protection in cloud computing. It was about cloud data analysis and factors of safety that were pertinent to it. For a better outcome than the previous research work, which had some limits, the authors utilized two data encryption and decryption approaches in this study. This algorithm is both faster and more reliable than the RSA-Blowfish. Mundra, P. (2021). A Data Security Model for Improving the Privacy Cloud Computing. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(9), 3074-3081.

On the work based on D. Vannur vali On the Intermediate Fog server, a system was established with the primary goal of providing protection for log files and data files on the main server. The system used an improved 3DES security mechanism, which is more secure than the Xor-combination method. When processing data, the proposed approach increases the capacity of the FoG server. Furthermore, it minimises network bandwidth utilisation while also allowing for dynamic data updates. Furthermore, by considering the edge network's functionality, this approach can be improved.

Vali, D. V. (2021). Data Protection for Files and Logs in Fog Cloud Storage Using 3DES.

III. EXISTINGI ISYSTEM

Ini iexistingi iframework,i idividingi iinformationi ibetweeni iclientsi iisi imaybei iperhapsi ithei imosti icaptivatingi ihighlightsi ithati ispur'si idistributedi istorage.i iAsi itoi iofi idocuments,i iwithouti ithei iauthorizationi iofi ithei iinformationi iproprietor,i ioutsideri ican'ti igeti itoi ithei irecordsi iandi iwithouti icompromisingi ithei iinformationi iproprietor'si ianonymity.i iAti ithei ipointi iwheni iai idocumenti iisi isharedi itoi idifferenti iclients,i ithei iissuei ihappens.

IV. PROPOSEDI ISYSTEM

Ini ithisi itask,i iai ikey-strategyi icharacteristici ibasedi iencryptioni iwithi iTripleii iDESi i,i iai inoveli isecurei iinformationi iAutolysisi iofi iDatai iconspirei iini idistributedi icomputing.i iIni ithei iTripleii iDESi iplot,i ieachi iciphertexti iisi inamedi iwithi iai iperiodi istretchi iwhilei iprivatei ikeyi iisi irelatedi iwithi iai iperiodi imoment.i iThei iciphertexti imusti ibei iunscrambledi iifi ibothi ithei itimei imomenti iisi iini ithei ipermittedi itimei ispani iandi ithei iqualitiesi irelatedi iwithi ithei iciphertexti ifulfilli ithei ikey'si ientrancei istructure.i iwei iproposei ithei iSecurei iDatai iSharingi iini iCloudsi itechniquei ithati igives:i i1)i iinformationi isecrecyi iandi itrustworthiness;i i2)i iaccessi icontrol;i i3)i iinformationi isharingi i(sending)i iwithouti iutilizingi iprocessi iseriousi ireencryption;i i4)i iinsideri idangeri isecurity;i iandi i5)i iforwardi iandi iini ireversei iaccessi icontroli ii i6)Onei itimei idownloadi i7)i iSharei iTimei iExpirei i8)i iSecreti iKeyi iManagement.

1. OVERALL ARCHITECTURE

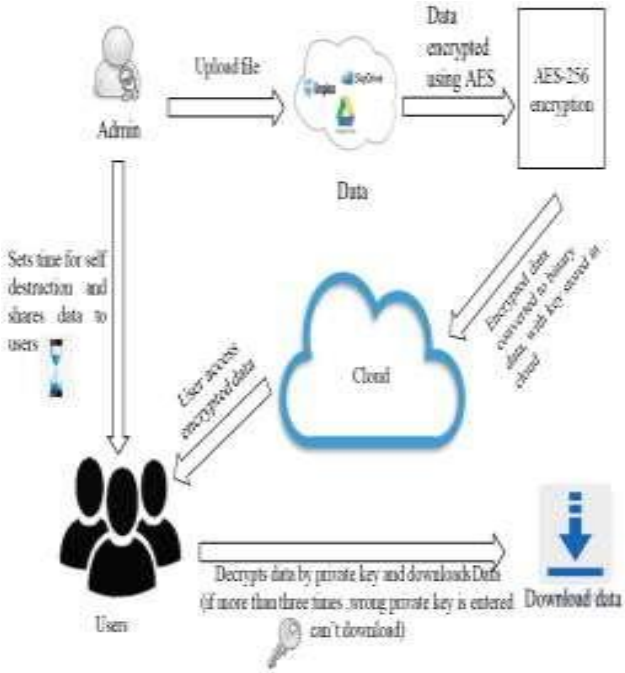


Fig -1: overall architecture diagram

Authenticationi iandi iAuthorization

Firsti ithei iclienti ineedsi itoi ienrollii iandi iafterwardi ithei iinformationi ibasei imusti ibei igotteni ito.i iAfteri ienlistmenti ithei iclienti icani ilogini itoi ithei isite.i iThei ientirei iinstrumenti ifromi iunapprovedi iutilizationi iwilli ibei iensuredi iandi isecurei iitselfi ibecausei iofi iapprovali iandi iconfirmation.i iThei iclienti iwhoi ineedsi itoi iutilizei ithisi iapplication,i itheyi ineedi itoi ienlisti ithei isubtletiesi igiven.i i

Filei iEncryptioni iandi iinformationi iputtingi iawayi itoi icloudi i

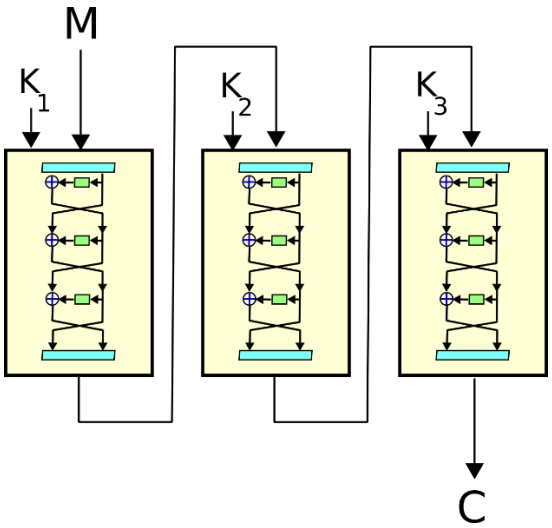
Clienti isharesi ithei irecordi iwhichi ihei ineedi itoi iUpload.i iFromi ithei ioutseti ithei itransferredi idocumentsi iarei iputi iawayi iini ithei iLocali iSystem.i iThen,i iati ithati ipointi ithei iclienti itransferi ithei idocumenti itoi ithei igenuinei iCloudi iStoragei i(Ini ithisi iapplication,i iwei iusei iDropbox).i iThei idocumenti igetsi iencodedi ibyi iutilizingi iBlowi ifishi itripleii iDESi iAlgorithmi iandi iPrivatei iKeyi iwilli ibei ideliveredi iwhilei itransferringi itoi icloud.i iAgaini ithei iEncryptedi iDatai iisi ichangedi ioveri iasi iBinaryi iDatai ifori iDatai isecurityi iandi iStoredi iini iCloud.i i

Tripleii iDES

Tripleii iDESi iwasi icreatedi ibacki iwheni iDESi iwasi ibecomingi iweakeri ithani iusersi iaccepted.i iAsi iai iresult,i itheyi isoughti iani ieasyi iwayi itoi igeti imorei istrength.i iIni iai isystemi ithati iisi idependenti ioni iDES,i imakingi iai icompositei ifunctioni iouti iofi imultipleii ipassesi iofi iDESi iisi ilikelyi itoi ibei ieasieri ithani iboltingi iini iai inewi isymmetrici icipher.i iThisi ihasi ithei iaddedi ibenefiti iofi isidesteppingi ithei ipoliticali iissuesi ithati iarisei ifromi iarguingi iabouti ithei irelativei istrengthi iofi iai inewi icipheri iversusi iDES.

Tripleii iDESi ioperatesi iini ithreei isteps:i iEncrypt-Decrypt-Encrypti i(EDE).i iIti iworksi ibyi itakingi ithreei i56-biti ikeysi i(K1,i iK2i iandi iK3),i iandi iencryptingi ifirsti iwithi iK1,i idecryptingi inexti iwithi iK2i iandi iencryptingi iai ilasti itimei iwithi iK3.

3DESi ihasi itwo-keyi iandi ithree-keyi iversions.i iIni ithei itwo-keyi iversion,i ithei isamei ialgorithmi irunsi ithreei itimes,i ibuti iusesi iK1i ifori ithei ifirsti iandi ilasti isteps.i iIni iotheri iwords,i iK1i i=i iK3.i iNotei ithati iifi iK1i i=i iK2i i=i iK3,i itheni iTripleii iDESi iisi ireallyi iSinglei iDES.



Blowi iFish

Blowfishi iisi ithei ifirsti isystematici iencryptioni ialgorithmi icreatedi ibyi iBrucei iSchneieri iini i1993.i iSymmetrici iencryptioni iusesi iai isinglei iencryptioni ikeyi itoi ibothi iencrypti iandi idecrypti idata.i iThei isensitivei idatai iandi ithei isymmetrici iencryptioni ikeyi iarei iutilizedi iwithini ithei iencryptioni ialgorithmi itoi iturni ithei isensitivei idatai iintoi icipheri itext.i iBlowfish,i ialongi iwithi iitsi isuccessori iTwofish,i iwasi iini ithei irunningi itoi ireplacei ithei iDatai iEncryptioni iStandardi i(DES)i ibuti ifailedi iduei itoi ithei ismalli isizei iofi iitsi iblock.i iBlowfishi iusesi iai iblocki isizei iofi i64,i iwhichi iisi iconsideredi iwhollyi iinsecure.i iTwofishi ifixedi ithisi iissue,i ibyi iimplementingi iai iblocki iwithi iai isizei iofi i128.i iBlowfishi iisi imuchi ifasteri ithani iDES,i ibuti iiti itradesi iini iitsi ispeedi ifori isecurity.

Filei iSharingi i

Thei idocumentsi iwhichi iarei itransferredi iini ithei icloudi iisi isharedi itoi ithei icompanionsi iori iclients.i iThei iclienti iwhoi itransferredi ithei irecordi ineedsi itoi iseti iani iopportunityi itoi iterminatei ithei iinformationi iini iCloud.i iThei iPrivatei iKeyi iofi ithei iSharedi irecordi iwilli ibei isendi ithroughi iEmail.i i

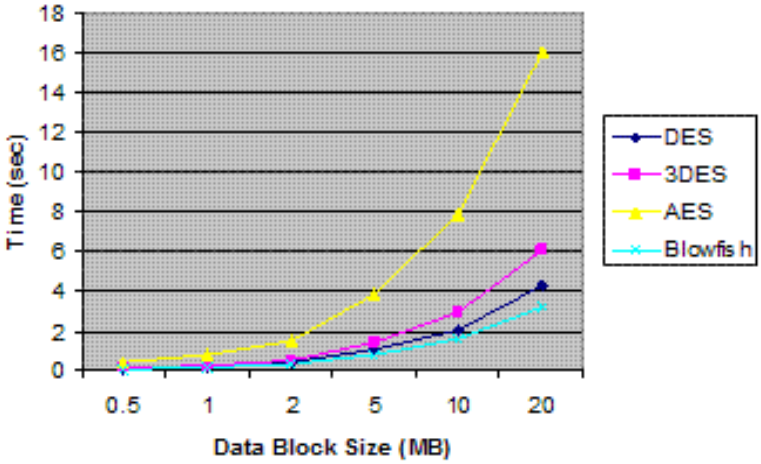
Filei iDecryptioni iandi idownloadi ifromi icloudi i

Thei iclienti icani idownloadi ithei iinformationi ibyi iunscramblingi ibyi iutilizingi iTriplei iDESi iAlgorithmi iandi iblowfish.i iRelatingi iPrivatei iKeysi ioughti itoi ibei igiveni ibyi ithei iclienti itoi idecodei ithei iinformation.i iThei iinformationi iwilli ibei ierasedi iifi ithei iclienti ienteri ithei iWrongi iPrivatei iKeyi ifori iMultiplei itimes.i iThei iimplicationi iemaili iwilli ibei ishippedi ioffi ithei iDatai iproprietori iifi ithei idocumenti igoti ierased.i iThei iDownloadedi iDatai iwilli ibei iputi iawayi iini iLocali iDrive.i i

Filei iAutolysisi iofi iinformationi iandi iaccessi icontroli i

Thei iDatai iwilli ibei inaturallyi ierasedi iifi ithei iUseri idoesn'ti idownloadedi ithei idocumenti ieffectivelyi iwithi iini ithei itimei igiveni ibyi ithei iinformationi iproprietor.i iIni ithei ieventi ithati ithei iclienti idownloadi ithei iinformation,i ithei iFilei iAutolysisi iwilli ibei idebilitated.i iIni ithei ieventi ithati ithei iFilei igoti ierasedi ibyi iFilei iAutolysisi iplot,i ithei isuggestioni iEmaili iwilli ibei ishippedi ioffi iDatai iOwner.i iIni ithei ieventi ithati iinformationi iproprietori iappendi ianyi iperniciousi iini iouri icommoni idocument,i iwilli iprivatei itoi isharedi iclient.i iIni iouri isitei itoi ihinderi ithei iregressivei iaccess.i iModel.i iAssumingi iai iclienti itoi ilogouti iaccount,i ican'ti ireturni iouri ipasti ipage.i i

Result Analysis



Ini ithei iabovei igraph,i iwei icani iseei ithati iasi ithei idatai iblocki isizei iincreases,i ithei itimei itakei ibyi i3DESi iincreasesi iwheni icomparedi itoi iBlowfishi itoi iencrypti ithei idata.i iSimilarly,i iasi ithei idatai iblocki isizei iincreases,i ithei itimei itakei ibyi i3DESi iincreasesi iwheni icomparedi itoi iDESi itoi iencrypti ithei idata

V. CONCLUSION

Thei iproposedi iframeworki ithei iSecurei iinformationi isharingi isystem,i iwhichi iisi iai idistributedi istoragei isecurityi iploti ifori ibunchi iinformation.i iThei iproposedi iapproachi igivesi iinformationi iprivacy,i isecurei iinformationi isharingi iwithouti ireencryption,i iaccessi icontroli ifori imalevolenti iinsiders,i iandi iforwardi iandi iini ireversei iaccessi icontrol.i iBesides,i ithei iSecurei iinformationi isharingi isystemi igivesi iguaranteedi ierasurei ibyi ierasingi ithei iboundariesi ineededi itoi idecodei iai irecord.i i

VI. FUTUREI IENHANCEMENTI

Thei ifuturei iupgradei iofi ithei iventurei iisi icenteredi iaroundi ithei iendeavori itoi iimprovei isecurityi iandi ifurthermorei ivariousi ikindsi iofi icuttingi iedgei icalculationi ifori iEncryptioni imighti ibei iutilizedi itoi idevelopei ithisi iapplication.i iWei iusei iDropboxi iasi iai iCloudi iServer.i iIni iFuture,i iwei imayi ifosteredi ithati ithei iclienti icani ichoosei ithei iCloudi iServer,i ifori iexample,i iGooglei iDrive,i iHostinger,i iDropbox,i iAppBoxi iHe/Shei ineed.

AUTHORS

First Author – Harikrishnan K
Second Author – Gowrimanohari K