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 iremovei iassociations iifromi ibuildingi iupi
iiin-housei iinformationi istockpilingi iframeworks.i
iNonetheless,i idistributedi istoragei ileadsi itoi isecurity
iconcerns.i iCloud-expliciti iandi itraditionali iiinsidei idangersi
iareai ilookedi ibyvi iinformationi iifii ifherei ieshouldi iarisei iani
ioccurrencei iiofif igatheringi iishedaredi information.i iThei
isignificanti iiuestei icii iii Securei idatii isharingi ibetweeni iai
igatheringi iihatii icounteresi iiinsidei idangersi iiiofainentici iyetii
ipermissionci iiclients.i iIIii ihithii iipaper,i iwei iiproseoi ithei
iSecurei iDataii iSharingii inii iCloudsii iiprocureii iihatii igives;i
i1) ii informationi ipriyaci iiani iiustroiwitfulness;i i2) ii acessei
icontrol;i i3) ii informationi isharingii i(sendii inwithout
iiutiliziingii iigeresi iseriousi iire-encryption;i i4) ii insidei iadangersi
isecurity;i iandii ii5) iiiforwardii iiani iiinverseii acessei iicontrol;i
i6) iiOneii itimeii i(idownloadii i7) iiShareii iiTimeii iExpireii i8) iiSecretii iKeyii iManagement;i iTheii iSecureii iinformationii
isharingii isystemii iencodei ii iarcodeii iwithii iisolitary
iencryptionii ikeyii.i iTheii iclientii igetsii ijustii iioneii idivideii
ibetweenii iiithii iidistinctiveii ikeyii iioffersii iiathai iareatedii
iifori ieveryii iiclientii.i iTheii iownershi piiii iiaii isolitaryai iportionii
iiofii iikeyii ipermitsii ithei iSecureii iinformationii isharingii
iprocureii iioi icounterii iiinsideii idangersii.i iTheii iothertii
ikeyii iofferii iiisii iii putii iiaawyii ibyii iiiaconfideii iiinsideii iioutsideii,
i iiwichii iiisii iiknownii iiathai icryptographici iworker;i iTheii
iSecureii iinformationii isharingii istrategyii iiisii iirrelevantii iiitii
icustomariy iiandi iiinverseii iiidistributedii icomputingii iconditions;i
iWei icarryri iioutii iiifunctioningii iiiofii iiithei iiSecureii iiidataii
isharingii iapproaci iiandi iiassessii iiisii ipresentationii iiependentii
ioni iiithei iiiieveooii iii duriii iidifferentii iactivities;i iTheii
ioutoucessii iiandi iiupii iiieingii iempowerigii iiandi iihowii iihatii
iSecureii iinformationii isharingii iiicanii iiioii iiequateai ilyii
iiutiliziiedii ifori iisecureii iinformationii iiapartakingii iiithii iicloud.
i

Index Terms- iiSecureii iidatii isharing, iiITripleii iiDES, iiiblowfiishii
ii, iirencrytion, iiKey, iiicloud.

I. INTRODUCTION

Distributed icomputingii ijoining iiiai biunchii iiofi iiexistiingii
iiandi iiinewii iiprocessuies iiormii iiresarchii iigriions, iiifori
ixample, iiadministriationii iiarrangedii iimodelsii ii(SOA)i iiandi
ivirtualizationii iiisii iconsideii iiiasi iiithii iiollowii iistageii iiini
iiithei iiidevelopiiiei iiiofii irquestii iidataii innovention,i iIII iiisii
istandardi iiifori iiicipantsii iiioi iidistributedii istorageii
iaadministriationsii iiioi imparati iii acontrolii iiioi iothersii iiiaii
iacompaniin iiicircle, iiicegii,i didroooxii, iigoegllee iiidriveii iaiiii
iCloud. iiTheii iicommonii iinformationii iiicloudii iworkers, ii
nonethless, iiitypically iiicontainii iiiclientsei iiouchyii idataii ii(eii, ii
iindividualii iprofile, iiimonetaryii iinformation, iiwellbeingii
irecords, iiandii isiioii iiandii iishouldii iieveryii iiumchi
isecured. iiAii iiithei iresponsibiliity iiifori iiinformationii isi
isolatedii ifromii iiithei iorganizationii iioclientii ihethem, iiithii iicloudii
iworkersii iiimayii iirelocateii iiiclientsei iiinformationii iiioii iothersii
icloudii iworkersii iiins eevaluatingii iiioffertii iithemii iiicloudii
iooking, iiIIii ihithse iiimanner, iiithii iilargeri iiestsii isi iirosenii
iiithei iprotectionii iiiofii ithoseii iicommonii iinformationii iiicloud, ii
iparticularii iini iiacross-cloudii iiandi ienormoussi iiinformationii
iiclimates, iiIIIii iiestsii icani ili imeti iiemetii iiimplanniingii iiiaii compleeti
iawserii iiiofii iheii ihichii iclientsei iiichertii iiaii iapproaaivi iiiperiod,
i iandii iiiti iiioteii iiiclientsei iiichertii iieterminationii iiitei
iiithei iicommonii iinformationii iiougthii iiioii iiactii inaturalii
iannihilitae, iiTheii iiinformationii isi iiupi iiiaayii iiiaii iiipically
iencodeii iestructurii iiioi iiightenii iiitsei iiisues, iiTheii iclientsei
iicantii ihisii/ierti iencodeii iiinformationii iiati iiifine-
gainedii ilevelii wiichii iiiaii ihindrancii iiiofii iscramblingii
information. iiTheii iiroprietori iihowldii iidefinii iiobjectiveii
isubtletiesii iiiofii iiiieoneii ihei/iheii ineedsii iiioii iiaparti iiatioii, iiIII ii
iinumerousii iappluccations, iiTheii iiinformationii iiroprietori iiinendsii
iiioii iiapartii idataii iiioi ifii ifeiwi iiiclientsei isi iiiicatedii iiibii iiitheii
iisecurityii istrategyii iidependentii iiioii iiiclientsei iiiiduelii,i
iiTheii icriticialii iibenefiti iiiofii iAttributii iibasedii iicryptionii
i(ABE)ii isi iiithii iiipendsii iiiofii iiicustomii iipublicii iikeyii
iicryptionii iartherii iiithii ibalancedii iiicryptionii isiinceii iiitii
iacomplishesii iiiadaaptableii ioneii to numerosii iicryption. iiTheii
tii iacomplishesii iboii iiuhii iiinformationii iiisecurityii iiandii iiifine-
gainedii iadmarntiice iicontrol, iiTheii iiicredibelii istrategyii isi
igiveni ibyi iITriplei iDES;i iplani iiandii ibloooii iiifshii iiicryptionii
icaulcalationii iiITripleii iDataii iEncrytiionii iiStandardii ii(iES)i iiiaii
iikindi iiiofii iiatoometii icryptographii iiwheeri iiisquaiii iiicdeii
icaulcalationsii iiareai iiappliedii iiimultipleii iiitmesii iiioii iieryii
iiinformationii iibloco, iiTheii iikeyii isiiei iiixexpandedii iiinii iiITripleii
iDES; iiitii iiiguaranteeii ixtraai iiisecurityii iithroughii iiicryptionii
icaucapiiicies, iiTheii iiisquaiii iiincludeii iiifii iiipesciiei iiiofii
information, iiTheii iiireeii iiareai iiialuidooodii iiioi iiapcki iikeyii
iiithii iiifii iiipescii iiiofii iiakeii, iiiblowfiishi iiiaii iiismetricii
iicryptionii iacaulation, iiimplyii iiitii iiutiliziess iiiaii iiisimilarii
iiisertii iiiysteryii ikeyii iiioii ibothii iiencodii iiandii iidodeii
iimagees, iiiblowfiishi iiiaii iiadditionalii iiiaii iiqareai iiode, ii
implyii iiitii iiisplitts iiiaii iiimagees iiintoi iiifixedii iielngthii
iblocksi iiirunii iiicryptionii iiandii iiunsrambling, iiTheii iiisquaiii
iielengthii iiifori iiiblowfiishi iiiaii iiiipennesii iiimagees iiiaii
iireciififiably iiinotii iiiaii iiidifferentii iiiofii iiieighet iiibytesii iiiaii iiisizeii
iiisohuldi iiimetii iiicushionedii,i iiAccordinii iiini iiithsei iiipaperii itei
iiinformationii isi iiareedii iisafelyii iiicloudii ithroughii

This publication is licensed under Creative Commons Attribution CC BY.
http://dx.doi.org/10.29322/IJSRP.11.11.2021.p11965
I. INTRODUCTION

Data security and privacy are becoming increasingly important as the amount of digital data continues to grow. The Internet of Things (IoT) and cloud computing have revolutionized the way we collect, store, and process data. However, these advancements have also introduced new challenges in terms of ensuring the confidentiality, integrity, and availability of data. This paper surveys the research in the area of data security in IoT frameworks, focusing on the use of elliptic curve cryptography (ECC) for secure data aggregation and transmission.

II. LITERATURE 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]


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]


The research of Debiao He et al., in the smart grid setting, proposed a lightweight 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].


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].


Sandep 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].


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]


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].


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].


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 framework. When comparing the standards used to secure communications, it was discovered that different approaches were employed to provide other security features [9].


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]


The work 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]


The works of Qinglei Kong et al., aimed 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]


The research done by Cheng Guo et al., offered a methodology that indicates the proposed approach has secured plain text assault resilience assault under the computational Diffie-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]


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 cipher 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]


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]


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]


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]


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. Mudra, 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.

III. EXISTING SYSTEM

Ini iexisting iframework,i idividingi informationi ibetweeni
clients iisi imaybei iperhapsi ithei imosts icaptivatingi
ihighlightsi ihtati ispur's iidistributed istorage.i iAsi itoi ifo
idocuments,i iwihoutti ithei iauthorizations iofi ithei informationi
ipropiotion,i ioutsiders iican't iigieti itoi ithei irecordsi iandi
iwihoutti iicompromisingi ithei informationi iipropiotion's iinionymity.i iAti ithei iipointi iwenhi iai idocuments iisi ishareddi
itoi idifferenti iclient,i ithei iissuei ihappens.

IV. PROPOSED SYSTEM

Ini ithiti itask,i ikey-strategy iicharacteristics iibasebi
ienceptioni iwithi iTriplei iDES,i iai inovel iisecurei
information,i iAutoysis ioi iData iiconsipri iini iidistributed
icomputing.i iIni ithei iTriplei iDES iiplot,i ieach iiciphertext iisi
inameddi iwidi iai iiperiodi istretcchi iwhilei iprivatei keyyi isi
iirelateddi iwidi iai iiperiodi imoment.i iThei iiciphertexti imusts iimbe i
iunscrambleddi ifi ibothi ithei itimei imomenti iisi ini ithei
ipermitteddi itimei ispandi iandi ithei iiqualitieds iirelateddi iwidi ithei
iciphertexti ifulfulldi ithei ikey'y isientrancei istructure.i iwei
iproposedi ithei iSecurei iData iSharingi iini iCloudsi iitechniqui
ithati igives:i i1) iinformationi iiesecredi ianddi iitrustworthiessu;i i2) iiacesssi icocontrol;i i3) iinformationi iisharindi isi (sendindi)
iwihoutti iutilizationi iprocesssi isericoius iirecryption;i i4) iiinsideri
iidayeri iisecurity;i iandi i5) iiforwardi iandi ini iivereversei iiacesssi
iicontrolsi ii6Oi nei itimei iiodownload i7) iSharei iTimei iExpiri
i8) iSecreti iKeyi iManagement.

1. OVERALL ARCHITECTURE

Authentication iandi iAuthorization

Firsti ithei iclienti ineedsi itoi ienrolli iandi iafterwardi ithei
iiformationi ibasei imusts iibe igotteni ito.i iAfteri ienlismenti
ithei iclienti ican'i iilogini itoi ithei isite.i iThei ientriiei iinstrumenti
ifiromi iunapprovedi itutilizationi iwilli iibe iensureudi iandi iisecurei
iitselfi iibecausei ioi iaiprovali iandi icomfirmation.i iThei iclienti
iwhoi ineessdi itoi itutilizei ithoii iapplication,i itheyi ineedi itoi
iienlisti ithei isubtletesi iigiven.i i

File: iEncryption iandi iinformation iiputting iawayi itoi
iicloudi i

Clienti isharesi ithei irecordsi ihichii ithei ineedi itoi iUpload.i
ifiromi ithei ioutseti ithei itransferedi idocuments iiarei iputi
iawayi ini ithei iLocali iSystem,i iTThen,i iani ihtati ipointi ithei
iclienti itransferi ithei idocuments itoi ithei iingenueini iCloudi
iStoragee i(iIni iithisi iappication,i iwei iuese iDropbox,i iThei
idocuments iigetsi iencodeedi iby iutilizationi iBlowi ifishi itriplei
iIDESii iAlgorithm iandi iPrivatei iKeyi iwilli iibe iodeliveredi
iwhilei itransferringi itoi iicloud.i iTAgaini ithei iEncryptedi iDatai
iisi ichangedi ioveri iasi iBinaryi iDatai ifori iData iisecuritiy iandi
iStoredi ini iicloud.i i

Tiiiplei iDES

Tiiiplei iIDESi iwasii icreatedi ibacki iwheni ini iDESi iwasii
iibecomingi iweakeri ihtani iusersi icpectedi iAsi iai iresulti,i
itheyi isoughti iani ieasyi iawayi itoi iigiets iionei istrength.i iIni iai
isystemi ithati isi independenti iioni iDES,i imakingi iicompositei
ifunctioni ioutti ioi iimultiplei ipasses iioi iIDES iisi iikelyi itoi
ithei ieasieri ihtani ioi iloltingi ini iai iinewi isymmetrici icipher.i
iThisi ihasi ithei iaddedi ibenefiti ioi iisdesteppingi ithei
ipiopoliticali iiissuesei itati iarisei ifromi iarguingi iabouti ithei
iirelativei istrengthi iofii iai iinewi icipheri iversusi iIDES.

Tiiiplei iIDESi ioperatesi iiini itthreei istespsei i1i iEncrypt-Decrypt-
Encrypti ii(EDE).ii iili iworksi ibyi itakingi iihereei i56-bit ikeysi
i(K1,i iK2i iandi iK3),i iandi iinceptioni ifirsti iwihith iK1,i
idecryptioni ineexti iwihith iK2i iandi iinceptioni iiai ilastsi itimei
iwihith iK3.

3DES ihasi itwo-keyi iandi ihtree-keyi iversions.i iini ithei
itwo-keyi iversion,i ithei iseami ialgorithm iirunsi ithreei itimes,i
iibuti iueseis iK1i ifori ithei ifirsti iandi ilastsi istesp.i iilni iiotheri
iwordsi,i iK1i isi iK3.i iNotei ihtati iifi iK1i is=i iK2i iis=i iK3,i itheni
iTiiiplei iIDESi isi ireallyi iSinglei iIDES.
Blowfish

Blowfish is a symmetric encryption algorithm created by Bruce Schneier in 1993. It uses symmetric encryption keys for encryption and decryption. The sensitive data and the symmetric encryption key are utilized with the encryption algorithm to encrypt data. Blowfish, along with its successors Twofish, is considered to be highly insecure. Twofish addressed this issue by implementing a block with a size of 128, which is faster than DES, but it also trades in its speed for increased security.

File iSharing i

The documents which are transferred in the cloud are shared by their companions or clients. The client who transferred the record needs an opportunity to terminate the information in iCloud. The private key of the shared record will be sent through Email. File iDecryption i

The client can download the information by unscrambling it by using Triple DES Algorithm and Blowfish. Relating to the Private key, the information is decrypted. Similarly, if the block size increases, the time it takes to encrypt the data also increases when compared to Blowfish which encrypts the data. Blowfish is faster than DES, but it is more secure in encryption and decryption.

File iAutolysis i

The data will be naturally erased if the iUser idoesn’t iupload the document effectively with inni iit/i the time the information is properly saved. iFile/i iAutolysis is a process where the data is deleted once the user logs out of the account. The data is erased once the user logs out. iModel/i iAssuming that the client is the log out account, i can’t ireturn to the user ipath ipage.

V. CONCLUSION

The proposed framework is a secure information sharing system which is distributed storage security plot for a bunch of information. The proposed approach gives information privacy, secure information sharing without encryption, access control if or malicious insiders, and ifoward and reverse access control. Besides, the Secure information sharing system is a user-friendly and secure iDrive, iHostinger, iDropbox, iAppBox, iHe/She ineed.

VI. FUTURE iENHANCEMENT i

The future upgrade of IoT devices is centered around IoT devices. It is more secure if the new version which is improved is improved. Furthermore, various kinds of iDevice iedge iCalculation ifor iEncryption iimight ibe iutilized iti idevices iithis iapplication. iWe use iDropbox ias iia iCloud/i Server. iIni iFuture, iwe iimay iifostered ithati iithi iiclient iican ichoose ithe iCloud/i Server, iifor iexample, iGoogle/i iDrive, iiHostinger, iDropbox, iAppBox, iHe/She ineed.

AUTHORS

First Author – Harikrishnan K
Second Author – Gowrimanohari K