SESPHR:AMETHODOLOGYFORSECURESHARINGOFPERSONALHEALTHRECORDSINTHECLOUD

G.Sreelekha[1],Sd.Ahmed[2]

[1]Assistant Professor, Dept of MCA, Audisankara College of Engineering & Technology(AUTONOMOUS),Gudur,AP, India.

[2]PGScholar, Dept of MCA,Audisankara CollegeofEngineering&Technology(AUTONOMOUS),Gudur, AP, India.

ABSTRACT

Thebroaduseofcloud-basedservicesinthehealthcareindustryhasmadeitpossibleforvariousparticipatingentitiesofthee-Healthsystemstoexchange personal health records (PHRs) at a lowcost and with ease. However, putting the privatehealth data on cloud servers leaves it open to theftordisclosure,necessitatingthecreationofproceduresthatprotectthePHRs'privacy.Consequently,wesuggestatechniquenamedSeSPHR for PHR cloud sharing that is secure. TheSeSPHRsystemmakessurethatPHRsarecontrolled from a patient- centric perspective andmaintainsthemaintainingthePHRs'privacy.Patients keep encrypted PHRs on unreliable cloudserversandonlygivecertainpeopleaccess.onvariousPHRsections,todistinctcategoriesofusers. a setup and re-encryption server, a semi-trustedproxy(SRS)isusedtocreatethere-encryptionkeysandtocreatethepublic/privatekeypairings.Additionally,theprocessissafe.It implementsaforwardandbackwardaccesscontroland protects against insider risks. Additionally, weofficiallyevaluateandconfirmtheuseoftheSeSPHRapproachusinghigh-levelpetrinets(HLPN). Evaluation of performance in relation totimeConsumptionsuggeststhattheSeSPHRapproachmaybeusedforsafelytransferringPHRstothecloud.

I. INTRODUCTION

Inordertoprovideubiquitousandon-demandavailability of different resources in the form ofhardware,software,infrastructure,andstorage,CLOUD computing has developed as a significantcomputing paradigm [1, 2]. As a result, the cloudcomputing paradigm helps enterprises by relievingthem of the time- consuming task of developinginfrastructureandencouragingthemtorelyonoutside Information Technology (IT) services [3].Additionally, the cloud computing architecture hasshowntremendouspromiseforimprovingcoordinationamongmanyhealthcarestakeholders andforguaranteeingscalabilityandongoingavailabilityofhealthinformation[4,5].Additionally,thecloudcomputingconnectsanumberofsignificanthealthcare domains,includingpatients,hospitalstaff,includingphysiciansandnurses,pharmacists,andclinicallaboratorystaff,aswellasinsurancecompaniesandserviceproviders[6].Asaconsequence,acollaborative and cost-effective health ecosystemwhere patients may easily establish and maintaintheir Personal Health Records (PHRs) develops asa result of the integration of the aforementionedorganisations[7].ThePHRsoftenincludedatalike:

(a) demographics, (b) medical history, includingdiagnoses, allergies, surgeries, and treatments, (c)laboratoryresults,(d)informationonhealthinsuranceclaims,and(e)patient-onlynotesregardingspecificsignificantobservedhealthissues [8].

Moretechnically,PHRsarecontrolledthroughInternet-based technologies, allowing individualsto manage their health information as permanentrecords that can be accessed by those who need it[9]. As a result, PHRs make it possible for peopletosuccessfullycommunicatewithmedicalprofessionals in order to describe their symptoms,ask for guidance, and maintain their health recordsforproper diagnosis and treatment.

Despitethebenefitsofthescalable,adaptable,affordable,andwidespreadservicesprovidedby the cloud, a number of issues linked to the privacyofhealthdataalsocomeup.Theuseofthecloudtodistributeandstore PHRsisacrucialfactorinpatients' concerns about the confidentiality of suchrecords [10]. Private health information stored oncloud servers run by third parties is vulnerable tointrusion. Particularly jeopardised is the privacy ofPHRskeptinpubliccloudsrunbyfor-profitserviceproviders [11]. The PHRs' privacy may be underdanger in a number of ways, including theft, loss,andleaking[12].Becauseofthemalevolentactionsofotherentities,the PHRsincloudstorage,intransit from the patient to the cloud, or from thecloudtoanyotheruser,maybevulnerabletounauthorisedaccess.Additionally,thereareoccasional threats made against the data by realinsiders [13]. For instance, due of the nefariousactions of other organisations, the PHRs in cloudstorage, in transit from the patient to the cloud, orfromthecloudtoanyotheruser,maybevulnerableto illegal access [10]. People who work for thecloud service provider may act maliciously. Theepisode in which a U.S. Department of VeteransAffairs employee took home without authority theprivatehealthinformationofover26.5millionpeopleisawell-known illustrationof that[14].

TheHealthInsurancePortabilityandAccountability Act (HIPAA) requires that patients'consent andthe terms of use anddisclosurebefollowedinordertomaintaintheintegrityandconfidentialityofelectronichealthinformationkept byhealthcareproviders[15].Additionally,thePHRs shouldbeencryptedwhenbeingkeptonthird-party cloud storage so that neither the cloudserverprovidersnorunauthorisedpartiesmayaccessthePHRs.ThePHRsshouldonlybeaccessibletoentitiesorpeoplewhohavethe"right-to-know"privilege.Topreventunauthorisedalterationsorabuseofdatawhenitistransferredtotheotherstakeholdersinthehealthcloudenvironment, the mechanism for granting access toPHRsshouldbemanagedbythepatientsthemselves.

TheprivacyofPHRskeptoncloudservershasbeenprotectedinavarietyofways.Confidentiality,integrity, authenticity,accountability, and audit trial are ensured by privacy-preservingmethods. While integrity concerns with preservingthe originality of the data, whether in transit or incloud storage, confidentiality guarantees that thehealthinformationiscompletelyhiddenfromunauthorisedparties[14].

Accountability refers to the need that data accessregulations follow the established protocols, whileauthenticity ensuresthat the health data isonlyaccessible by authorised parties. The term "audittrial" refers to the process of observing how healthdata is used even after access to it has been given[6].

We provide a way for managing the PHR accesscontrolsystemthatiscontrolledbypatients themselves, dubbed Secure Sharing of PHRs in theCloud (SeSPHR).

The approach limits unauthorised users to protectthePHRs'confidentiality.Inthesuggestedapproach,therearetypicallytwocategoriesofPHRusers: (a) patients or PHR owners; and (b) users ofPHRs who are not owners, such as patients' familymembers or friends, physicians, health insurancecompanyrepresentatives,pharmacists,and researchers.

By selectively providing people access to certainPHR sections, patients who are the PHRs' ownersareallowedtouploadencryptedPHRstothecloud.Depending on their job, each member of the groupof users of the latter kind is given access to thePHRs to a certain degree by the PHR owners. ThePHR owner defines the degrees of access given todifferent user groups in the Access Control List(ACL).

For instance, the owner of the PHRs may providecomplete access to the patient's family members oracquaintances. Similar to this, insurance companypersonnel would only be allowed to see the PHRsectionsthatincludeinformationconcerninghealthinsuranceclaims,withaccesstootherpersonalmedicalinformation,suchthepatient'smedicalhistory,beingblockedfortheseusers.

The SeSPHR methodology avoids the overhead bydelegatingtheSRSforsettingupthepublic/privatekeypairsandproducingthedecryptionkeysforthe authorised users only. In contrast to the approachproposedin[10],whichsuggeststhatthePHRownersmanagemultiplekeys,thisapproachavoidsoverheadbyproposingthatthePHRownersproduce the decryption keys. This ultimately leadstooverheadatthePHRowner'send.TheSetupand Reencryption Server (SRS), a semi-trusted server,isusedastheproxysincetheapproachviewscloudserversasanuntrustedentity.FortheSRStogenerate the re-encryption keys for safe sharing ofPHRsacrossusers,aproxyreencryption-basedtechniqueisutilised.PatientsorPHRownersencrypt the PHRs, and only authorised users withkeys provided by the SRS may decode the PHRs.Additionally,theusersaregivenaccesstothePHRs'particularsectionsthatthePHRownerdeemstobecrucial.Theproposedmethodissecurecomparedtopreviousconstructssincethe PHRdataisneversentfromthe SRSintheproposedframework.Instead,itistheSRS's dutytomaintainthe keys, with PHR owners handling encryptiontasks,andrequestingusershandlingdecryptiontasks,providedtheyhaveaccesstovaliddecryptionkeys.

Theforwardandbackwardaccesscontrolsarelikewise enforced by the suggested method. Thekeysareobtainedbythenewlyjoiningmembersofacertainusergroupfromthe SRS.Onlytheowner'skeys areusedto encryptthe shared data. After receiving the PHR owner's consent, newlyjoining members are given access to the data. Thecorresponding keys for a departing user are alsodestroyed, and that user is also removed from theACL.Anyunauthorisedaccessattemptsmadeafter the user has left are denied access to the PHR dueto the deletion of the user keys and removal fromthe ACL.WealsousedHighLevelPetriNets(HLPN)andtheZlanguagetodoaformalexaminationofthesuggesteddesign.

TheHLPNisusedtobothimitatethesystemandtoprovide the mathematical characteristics that arelaterutilisedtoanalysethebehaviourofthesystem. TheZ3solverandtheSatisfiabilityModuloTheories Library (SMT-Lib) are used to carry outtheverification.Tocarryouttheworkofverification using the SMT, the petri net model isfirsttranslatedintotheSMTtogetherwiththespecified properties, and then the Z3 solver is usedtocheckwhethertheproperties aretrueorfalse.

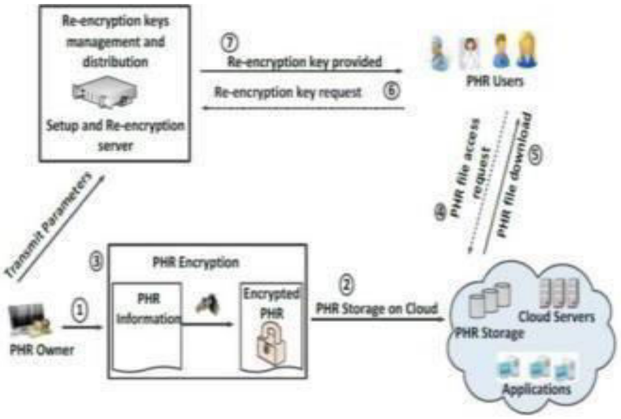

Fig-1:ArchitectureoftheproposedSeSPHRmethodology

The following are the main contributions of thesuggestedwork:

1. SeSPHR, a technique we offer, enables patientsto control the sharing of their own PHRs in thecloud.

2. TomaintainPHRsecrecy,theSeSPHRapproachusesproxyre-encryptionandEl-Gamalencryption.

3. Based on the access level established in the ACLfor various user groups, the approach enables PHRowners to selectively provide users access to usersoverthesectionsof PHRs.

4. To provide access control and to produce thereencryption keys for various user groups, a semi-trustedproxynamedSRSisimplemented,removing the burden of key management from thePHR owner'send.

5. The suggested technique also uses forward andbackwardaccesscontrol.

6. Thesuggestedapproachisformallyanalysedandverifiedtoensurethatitoperatesinaccordancewiththerequirements.

II. RELATEDWORK

The existing works that are related to the proposedwork are presented in this section. By sending thePersonallyIdentifiableInformationindividually,theauthorsin[28]developedapublickeyencryption-basedtechniquetomaintaintheanonymityandunlinkabilityofhealthinformation in a semitrusted cloud (PII). The Cloud ServiceProvider(CSP)savesthe healthrecordandthelocation of the file (index), and later encrypts themusingsymmetrickey encryption.

ThepatientsencryptthePHRsbythepatientsusingthepublickeyoftheCSP,andtheCSPdecryptstherecord using the private key. By associating thelocationandthemasterkey,theadministrativecontrol of the patient on the PHRs is kept in place.The approach's drawback is that it enables the CSPtodecryptPHRs,whichmaythenbeusedmaliciously.TheSRS,ontheotherhand,isasemi-trustedauthoritythatdecryptstheciphertextcreatedby thePHRownerandprovideskeystotheusers thatrequestaccesstothePHRs.

Inamulti-usercloudsetting,Chenetaltechnique.'s [12] uses the SKE and the Lagrange Multiplier todynamically exercise access control on PHRs. Theapproach'sprimarycharacteristicsincludeautomaticuserrevocation.Apartialorderlinkbetween the users is kept in order to get around thechallengesofotherkeymanagement.However,the systemrequiresthePHRowners'onlinepresenceinordertogiveorcancelaccess.Oursuggestedtechnique does not need the PHR owners to beonline in order to offer the access over PHRs, incontrast to the plan described in [12]. Instead, thesemi-trustedauthoritychoosestheusers'accessrightsand,uponsuccessfulauthorisation,decides the re-encryption keys for the users making therequest.

Toprovidepatient-centricaccesscontrol,theauthorsin[29]developedaDigitalRightManagement (DRM)-based solution. The writersusedContentKeyEncryption(CKE)toencrypt thedata,andonlyuserswithvalidlicencesareallowedaccess.Thefirstproxyre-encryptiontechniquewasputoutin[33].Unlikeourpolicy,whichisbasedonkeysandhasnoeffectonthesizeof theciphertext,the policy in [33] is based on ciphertext, and thesize of the ciphertext rises linearly with multi-useusage. This is because the [33] needs a step that ismissing from our methodology—re- encryption. Lietal.[14]offeramethodforsharingPHRsinmulti-ownersettingsthatareseparatedintoseveraldomainsthatusesattribute-basedencryption(ABE).

The technique initially presented in [33] serves asthefoundationforthesuggestedmethodology.After a given user's access has been revoked, themethod re-encrypts the PHRs using the proxy re-encryptionmechanism(s).Themethodsuccessfullyreducesthecomplexityandexpenseofkeymanagement whilealsoimprovingthephenomena of on-demand user revocation. Despitebeingscalable,themethodisunabletohandlesituations when granting access permissions basedonusers' identities is necessary.

To guarantee user responsibility, Xhafa et al. [30]also applied Ciphertext Policy ABE (CPABE). Inaddition to preserving user privacy, the suggestedmethod has the ability to track down users whomisbehaveandillegitimatelysharetheirdecryptionkeys with other users.

It presents a method for ensuring both the secrecyand fine-grained access to the healthcare data thathas been contracted out to cloud servers. By usingproxy re-encryption, Key Policy ABE (KP-ABE),and lazy re-encryption, the expensive duties of re-encryptingdatafiles,updatingsecretkeys,andpreventing users whose access has been revokedfrom learning the contents of the data are handled.There-encryptionofdatafilesandsubsequentstorageinthecloudenvironmentareresponsibilitiesassignedtothecloudservers.However, the data owner is also expected in theproposed framework to be a reliable authority whocontrols thekeys forseveralowners andusers.

Therefore,managingseveralkeysforvariousattributes for many owners would be inefficient atthePHRowners'end.Becausethefunctionsofkeycreation and key distribution to various user typesare carried out by the semi- trusted authority, ourtechnique eliminates overhead. In order to providefine-grained accesscontrol, the authorsin[31]and [32]alsoemployedproxyre-encryption-basedtechniques. The system we provide allows

ownerstoencryptPHRsbeforeputtingthemintheclou
d

and adds a semi-trusted authority that re-encryptsthe ciphertext without knowing what's within thePHRs.ThePHRscanonlybedecryptedbyauthorisedusers whopossessdecryptionkeysissuedbythesemi-trustedauthority.

III. PROPOSEDMETHODOLOGY

The recommended method makes use of proxy re-encryptiontoprovidePHRconfidentialityandexchangesecurityacrosspublicclouds.Thearchitecture of the suggested SeSPHR technique isshownin Fig. 1.

Persons the recommended method for exchangingPHRs in a cloud environment involves the SetupandRe-encryptionServer(SRS),thecloud,andtheusers.Anoverviewofeachoftheentitiesisprovidedbelow.

ThecloudThestrategyadvisesPHRownerstosavetheir data in the cloud so they may subsequentlysafely share it with other users. Users assume thatthe cloud is an unreliable source when they uploador download PHRs to or from cloud servers. NochangestothecloudarenecessarysincebothtypesofusersaretheonlyonesthatuploadanddownloadPHRs in theway stated.

Setting up and installing the SRS: Every systemuser'spublic/privatekeypairsmustbegeneratedbythe SRS, a semi-trusted server. The SRS furthergenerates the re-encryption keys in order to safelytransferPHRamongseveralusergroups.TheSRS isregardedasasemitrustedentityintherecommended method.Inlightofthis,wedrawtheconclusion that it is honest and generally followsthelaw,butodd.TheSRSmonitorsthe keys,butitnevergetsPHRinformation.Operationsfor encryptionanddecryptionarecompletedattheendpointsoftheusers.TheSRSofferskeymanagement in addition to access control for theshareddata.

Dueofthepubliccloud'sunreliability,theSRSisastandaloneserverthatcannotbeinstalledthere.TheSRS may be managed by a group of institutions orby a respectable third-party organisation forthebenefit of the patients. It could also be maintainedby a group of connected patients. However, SRSmaintainedbyhospitalsoragroupofpatientsmightinspirehighertrustduetotheinvolvementofmedical specialists and/or the patients' self-controlover SRS.

Users:Patients(ownersofPHRswhowishtosecurelysharetheirPHRswithothers)andpatients'familymembersorfriends,doctors,representativesof health insurance companies, pharmacists, andresearchers are the two main groups of users of thesystem. Friends and relatives are classed as privatedomainusersundertheSeSPHRmethodology, whereas all other users are categorised as publicdomainusers.

PHR owners may provide users access to PHRs inthepublicandprivatedomainstovaryingdegrees.

Userswhocomeundertheprivatedomain,forexample , may have complete access to the PHR,butthosewhofallunderthepublicdomain,suchasphysicians, scientists, and pharmacists, would onlyhave access to a limited number of PHR parts. Theaforementionedusersmayalsobegrantedfullaccess to the PHRs if the PHR owner determines itis required. In other words, the SeSPHR approachallows patients to impose precise access controlover PHRs.

Every system user must register with the SRS inorder to access the SRS's services. As a doctor,researcher,orpharmacist,forexample,theregistration procedure is dependent on the user'sresponsibilities.

HRPartitioning

The four sections listed below are logical divisionsof thePHR:

Personalinformation,health-relatedinformation,insuranceinformation,andinformationonprescriptiondrugs;

Itiscrucialtonotethattheaforementioneddivisionis flexible. The PHR may be divided into fewer ormore divisions at the user's discretion. The PHRsare represented in a number of formats, includingXML,andmaybesimplyseparatedintopieces.ThePHR owner also has the option of giving manypartitions the same level of access control. SomePHRpartitionsmayincludeuserrestrictions, meaning that a particular user may not have fullaccess to thehealth data.

For instance, a pharmacist may not have access topersonal or medical information, but they may begivenprescriptionandinsurance-relatedinformation. Full access to the PHR may also begiven to family members and friends. A researchercouldonlyneedaccesstothepatient'smedicalrecords once the personal data has been deleted.The PHR owner grants the SRS access rights toeach of the various PHR partitions when data isuploadedtothecloud.

TheProposedMethodology'sApproachFunctions

The suggested SeSPHR technique consists of thefollowing steps: setup, key creation, encryption,and decryption. The parts that follow go througheachaction:

SETUP

The offered approaches work well with the G1 andG2 groups with the prime order q. G1 G1G1 andG2 are bilinearly mapped to form G2. A randomnumbergeneratorwheregG1hasgasaparameter.Z is used as a second random number generatorusingtheformulaZ= e(g, g) G2.

KeyGeneration

Public/privatekeypairsarecreatedbytheSRSforthesetof authorised users.

ENCRYPTION

Imagine that patient P is required to upload theirPHR to the cloud. The PHR partitions that the userhasallocatedtothedifferentaccesslevelgroupsarerepresented by a random number or numbers thatare generated by the patient client application. Inour case, we take into consideration that the accesslevels for each of the four partitions specified inSection 3.2 vary. As a consequence, four randomvariables are created in our example: r1, r2, r3, andr4 (Zq). The variable ri is used to encrypt the i-thpartition of the PHR. Each partition is encryptedseparately by the client programme. Thanks to theXMLstructure,theapplicationcanquicklyperform encryptionanddecryptiononthe PHR'slogicalpartitions. The partitions stated above in the PHRareencryptedasseenbelow.

The quantity of PHR partitions; the titles of eachpartition,suchas"PersonalHealthRecord"(PHR),"MedicalRecord,""InsuranceInformation,"and"PrescriptionInformation;(anyrolemaybegrantedaccess to more than one partition, such as doctorsmaybegrantedaccesstomedicalinformation).

- The first close relative or acquaintance toprovide access • If there is any default access fornew members

DECRYPTION

Let's assume user U requests access to the patientP'sprovidedencryptedPHR(C).UserUdownloadsthe C directly from the cloud after completing thecloudauthenticationprocess.TheuserUrequests the SRS to determine and deliver the correct Rparametersrequiredfordecryptionatthatpoint.Bylookingattheaskinguser'sACL,theSRSdetermines if the PHR owner has granted access tothe partition for which the user has requested R.BasedontheaccessrightsspecifiedintheACL,theSRSwillcreateandprovidethenecessaryparameters to the requesting user. We shall showhowRisproducedforeachdivisioninthetextthat followsinordertoprovideacomprehensiveexplanationoftheprocedure.Therefore,weassumethat user U has complete access to all partitions.The SRS computes R and sends it to the user Utogetherwiththere-encryptionkey.

VI.CONCLUSION

We suggested a mechanism for transmitting andstoring PHRs in the cloud securely to authorizedparties.Thetechniqueupholdsapatient-centricaccesscontroltovariousPHRsubsystemsbasedontheaccessgrantedbythepatients,whilemaintainingtheprivacyof thePHRs.

Weputinplaceaformoffine-grainedaccessrestriction so that not even authorized users of thesystem could access restricted areas of the PHR.Onlyauthoriseduserswithlegitimatere-encryption keys supplied by a semi trusted proxyareabletodecryptPHRs,whicharestoredencrypted by PHR owners in the cloud. The tractortrailer proxy's job is to create and maintain publicandprivatekeypairsforthesystem's users.

Themethodologyalsomanagesforwardandbackward identitymanagementforleavingandnewlyjoiningusers,correspondingly,inadditiontomaintainingconfidentialityandguaranteeingpatient-centricaccesscontrolforPHRs.Additionally, we officially assessed and validatedtheSeSPHRmethodology'soperationusingtheHLPN,SMT-Lib,andZ3solver.Thetimeittooktogeneratekeys,theactivitiesinvolvedinbothencryptionanddecryptionincludingtimelydeliverywasalltakenintoaccountwhenevaluatingperformance.Theoutcomesoftheexperiment show that the SeSPHR approach maybeusedtosafelyexchangePHRsinacloudcontext.

V.REFERENCES

[1] K.Gai,M.Qiu,Z.Xiong,andM.Liu,“Privacy-preserving multi-channel communicationin Edge-of-Things,” Future Generation ComputerSystems,85, 2018, pp.190-200.

[2] K. Gai, M. Qiu, and X. Sun, “A survey onFinTech,”JournalofNetworkandComputerApplications,2017, pp. 1-12.

[3] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan,“Acloudbasedhealthinsuranceplanrecommendationsystem:Ausercenteredapproach,“Future Generation Computer Systems, vols. 43-44, pp. 99-109, 2015.

[4] A.N.Khan,MLM.Kiah,S.A.Madani,M.Ali,andS. Shamshirband,“Incrementalproxyre-encryptionschemeformobilecloudcomputingenvironment,”TheJournalofSupercomputing,Vol.68,No.2,2014,pp.624-651.

[5] Srikanth veldandi, et al. “An Implementation of Iot Based Electrical Device Surveillance and Control using Sensor System.” Journal of Energy Engineering and Thermodynamics, no. 25, Sept. 2022, pp. 33–41. https://doi.org/10.55529/jeet.25.33.41.

[6] Srikanth veldandi, et al “Design and Implementation of Robotic Arm for Pick and Place by using Bluetooth Technology.” Journal of Energy Engineering and Thermodynamics, no. 34, June 2023, pp. 16–21. https://doi.org/10.55529/jeet.34.16.21.

[7] Srikanth, V. “Secret Sharing Algorithm Implementation on Single to Multi Cloud.” Srikanth | International Journal of Research, 23 Feb. 2018, journals.pen2print.org/index.php/ijr/article/view/11641/11021.

[8] V. Srikanth. “Managing Mass-Mailing System in Distributed Environment” v srikanth | International Journal & Magazine of Engineering, Technology, Management and Research, 23 August. 2015. http://www.ijmetmr.com/olaugust2015/VSrikanth-119.pdf

[9] V. Srikanth. “SECURITY, CONTROL AND ACCESS ON IOT AND ITS THINGS” v srikanth | INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING, 15 JUNE. 2017. http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170605.pdf

[10] V. Srikanth. “ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS” v srikanth | INTERNATIONAL JOURNAL OF MERGING TECHNOLOGY AND ADVANCED RESEARCH IN COMPUTING, 20 MARCH. 2017. http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

[11] V. Srikanth. "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION" v srikanth | INTERNATIONAL JOURNAL OF INNOVATIVE ENGINEERING AND MANAGEMENT RESEARCH, 08 DECEMBER. 2017. https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

[12] V. Srikanth. "SECURED RANKED KEYWORD SEARCH OVER ENCRYPTED DATA ON CLOUD" v srikanth | INTERNATIONAL JOURNAL OF INNOVATIVE ENGINEERING AND MANAGEMENT RESEARCH, 08 Febraury. 2018. http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

[13] V. Srikanth. "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)" v srikanth | Journal of Emerging Technologies and Innovative Research (JETIR), 08 mAY. 2019. https://www.jetir.org/papers/JETIRDA06001.pdf

[14] V. Srikanth, et al. "Detection of Fake Currency Using Machine Learning Models." Deleted Journal, no. 41, Dec. 2023, pp. 31–38. https://doi.org/10.55529/ijrise.41.31.38.

[10]

[15] "Health Insurance Portability and Accountability," http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/,accessedonOctober20,2014.

[16] Z. Xiao and Y. Xiao, "Security and privacyincloudcomputing,"IEEECommunicationsSurveysandTutorials,vol.15,no.2,pp.1–17,Jul.2012.

AUTHORS PROFILE

G.SREELEKHAis currentlyworkingasAssistantProfessorinAudisankaraCollegeofEngineering&Technology(AUTONOMOUS),NH-5, BypassRoad, Gudur,Tirupati(Dt.),AndhraPradesh, India.

SD. AHMED is pursuing MCA from Audisankara College of Engineering & Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India