iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71720

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Design of an Efficient and Secure Smart City Framework Using Blockchain

Bogaraju Archana[1], Malakadi Spandana[2], Bolli Vijith Kumar[3], Mr.CH.Gopi[4]
[1, 2, 3]*Students,* [4]*AssistantProfessor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, INDIA*

Abstract: ***Building smart services for smart cities has become a major focus in modern technological advancements. Mobile scanners play a crucial role in capturing and processing data from various sources. Smart city applications emphasize the need for secure data sharing across heterogeneous devices. However, certain actions taken during data sharing can pose risks to security, privacy, and data integrity. The reliance on a centralized repository has been a major factor in past securitybreaches. Therefore, ensuringsecureauthenticationand the protectionof sensitivedata is crucial formodern applications. Blockchainisawidelyadoptedtechnologythatensuresdataintegrityandsecurity.Thispaperintroducesanovelblockchainbasedframework,SecPrivPreserve,designedtoenhancethesecurityandintegrityofdatageneratedbymobilescanners.Theproposedframeworksecures datathroughmultiplephases,includinginitialization,registration,dataprotection,authentication,accesscontrol,validation,datasharing,andsecuredownloads.Tostrengthensecurity,SecPrivPreserveintegratesvariousmechanismssuchasencryption,hashing,andauthentiationtechniquesthatenhanceconfidentiality,privacy,andintegrity.Unliketraditional approachesthat rely on one-time passwords(OTP) for authenticationand data sharing,this frameworkemploys QR codesforsecureaccessand datasharingkeystofurtherenhancesecurity.SincetheSecPrivPreserveframeworkisbuiltonapermissionedblockchain,itinherentlybenefitsfromtamper-proofrecordsandnon-repudiation.Moreover, for data protection techniquesto enhance cryptographicsecurity.***
Keywords: SHA256,Blockchain,CryptoGraphicTechniques,Authentication,SmartContract

I. INTRODUCTION

Recently, all the nations in the world have been gearing up their services, applications, and infrastructure for the betterment of their people's life using smart technologies. In this context, the Internet of Things (IoT) is crucial for connectingphysicaldevices totheinternetusingdifferentprotocolstofacilitatedatatransferamongdiverseplaces. In recent decades, there has been an enormous necessity for IoT-based services in various sectors such as healthcare, manufacturing,financialservices, trafficmonitoring, weathermonitoring,andenergytransfer.Duetotheircompactnessandminimalpowerconsumption,theusageofIoTdevicesisexpectedtoreachmorethan$1.4trillion in 2027. Many countriesinvest a lot of money in initiativesrelatingto smart cities. For instance, Chinais engaged in more than 220 initiatives that aim to create a smart city and improve the quality of life for citizens. Associated technologiesforsmartcitiesassisturbanmunicipalitiesinmanagingtheirday-to-dayoperations.AccordingtoIBM, the smart city has three main characteristicsinstrumented(sensors, actuators),interconnected(informationsharing among devices), and intelligent (improve quality of citizens' life). Recent observation reveals that the smart city has substantially enhanced the quality of life and amenities of inhabitants in urban areas. According to a United Nations Population Fund report, more than half of the world's population lives in urban areas. The smart city has caught the attention of both academia and business since it has significantly decreased the logistical problems related to acquiring services. Severalcitiesworldwidehave begunto build theirown smartcity strategiesto improvetheir inhabitants' qualityoflife.IoT andsmartenvironmentshavebecomesynonymous.IoTtechnologyiscapableofsensingevery entityinthereal world, soitfindsimportanceinhealthcare,transport,trafficsystem,publicsafety,smartbuilding, and smart agriculture. Amid many merits, due to the presence of inconsistent protocol standards, resourceconstrained nature, and centralizedrepository IoT devices are vulnerableto security and privacy breaches. In a smart environment, peoplemayfacesecurity andprivacyrisksdue tothevulnerabilitiesinsmartcity applications. For instance, malicious attackers may fabricate data to execute their ill intent, which may jeopardize the decision-making system. In addition, these malicious attackers also make all sorts of attempts to prevent the legitimate users' service by executing denial-of-service(DoS) attacks, transmission, disrupting sensing, and control in order to degrade the quality of intelligentcity services. Furthermore, as new devices or software are connected, the complexity level of the risks of smart city applications grows, particularly while ensuring privacy. Unfortunately, most protection methods (encryption, authentication mechanism) are insufficient to protect smart city applications against the new dynamic threats.

©IJRASET: All Rights are Reserved

Implementing complex procedures wouldn't be possible since the devices have less computational power.Hence,asimpleframeworkthatconsiderssimplecryptographytechniqueswouldbeanappropriatesolution for IoT's heterogeneity and dynamic characteristics is appreciable. Data breaches can occur during data storage, transmission,andsharing, posingsignificantriskstodataownersandproviders.Regulationsareinplacetoprotectthedatasourceandthesystemfrompotentialharmcause dbytargetdatanodes.Asaresult,duringdatatransactions, it is imperative that both the source and target nodes comply with the policies and regulations of their respective areas. Smart cities are built around integratingsensors and smart technologies,allowingcitizens and organizations to access datathroughtheirsmartdevicesto processandutilizedata.However,theutilizationof datainsmartcitiesraises privacyconcerns,includinghacking sensitivedata throughinjectingdata poisoningattacks.These attackscouldresult in the alteration of sensitive data, which in turn leads to the disruption of communication within smart entities. IoT networksinsmartcitiesareparticularlysusceptibletocyber-attacksthatthreatenthedataintegrity,confidentiality, and availability of these systems. To mitigate these risks, smart cities must implement robust security mechanisms to protecttheirassetsagainstcyber-attacks(DistributedDenialofService(DDoS),DoS,ManintheMiddle,ransomware).Thefrequencyandimpactoftheseattacksemphasizethe needforadequateprivacyandsecurity measures in smart cities. Researchers have developed many data-securing schemes to offer privacy and security for applicationsmeantfor smartcities.Earlier centralizedcloud-baseddata-sharingframeworkshave failed toaddress smartapplications'dataintegrityandprivacyissues.However,blockchain-basedsolutionsprovidegreater improvementin solvingprivacyissues.Initially,data collectedfromsensorsusinga detectionalgorithmtakesclient data into various communities based on similarity labels. It has a specific type of control on community data with specifyingdetectionalgorithm. However,thisframeworkhasnotaddresseddataprotection.

II. LITERATURE SURVEY

1) Title: AreviewofsecurityvulnerabilitiesinIndustry4.0applicationandthepossiblesolutionsusingblockchain.
Author:M.Ramaiah,V.Chithanuru,A.Padma,andV.Ravi.
Year:2023.
Description:
Industry 4.0 is a technology initiative intended to improve the efficiency of the task for the smart manufacturing industries.Industry4.0encompassesthetrendingtechnologieslikeIntheInternetofThings,IndustrialInternetof Things, Artificial Intelligence, and Big Data analytics and comes up with their challenges while customizingit for the task. Trendingsmarttechnologiesare no exceptionto being hackedby cybersecurityattacks. To facilitate automation, theinterconnecteddevicesneedrobustandintelligentsecuritysystemstopreventsecuritybreachesanticipatedfrom theanonymousentity. Hence,a clearunderstandingof varioussecurityaspectsofIndustry4.0 isveryessentialto preventsecurity attacks.This chapterattemptsto highlightthepossiblesecurityvulnerabilitiesanticipatedforIndustry4.0fromitsconstituentkeyelementsandthepossiblesecuritysolutionusi ngblockchaintechnologies.

2) Title: VeDB:AsoftwareandhardwareenabledtrustedrelationaldatabaseAuthor:X.Yang,R.Zhang,C.Yue,Y.Liu,B.C.Ooi,Q.Gao,Y.Zhang,andH.Yang,
Year:2023
Description:
Blockchain-like ledger databases emerge in recent years as a more efficient alternative to permissioned blockchains. Conventionalledgerdatabasesmostlyrelyonauthenticatedstructuressuchastheirkletreeandtransparencylogs for supporting auditability, and hence they suffer from the performance problem. As opposed to conventional ledger DBMSes, we design VeDB - a high-performance verifiable software (Ve-S) and hardware (Ve-H) enabled DBMS with rigorous auditability for better user options and broad applications. In Ve-S, we devise a novel verifiable Shrubs array (VSA)withtwo-layerordinals(serialnumbers)whichoutperformsconventionalMerkletree-basedmodelsdue to lower CPU and I/O cost. It enables rigorous auditability through its efficient credible timestamp range authentication method, and fine-grained data verification at the client side, which are lacking in state-of-the-art relational ledger databases.InVe-H,wedeviseanon-intrusivetrusted affiliationbyTEEleveragingdigestsigning,monotonic counters, and trusted timestamps in VeDB, which supports both data notarization and lineage applications. The experimentalresultsshow that VeDB-VSAoutperformsMerkletree-basedauthenticated datastructures(ADS) up to 70×and3.7×forinsertionandverification;andVeDBVe-Hdatalineage verificationis 8.5×fasterthan Ve-S.

3) Title:Privateblockchainenvisionedaccesscontrolsystemforsecuringindustrial IoT-basedpervasiveedge computing.
Author:S.Saha,B.Bera,A.K.Das,N.Kumar,S.H.Islam,andY.Park.
Year:2023
Description:
The Industrial Internet of Things (IIoT) is able to connect machines,analytics and people with IoT smart devices,gateway nodes and edge devices to create powerful intuitivenesses to drive smarter, faster and effective business agreements. IIoT having interconnected machines along with devices can monitor, gather, exchange, and analyze information. Since the communication among the entities in IIoT environment takes place insecurely (for instance, wirelesscommunicationsandInternet), anintrudercaneasilytamperwiththedata. Moreover,physicaltheftof IoT smartdevices providesanintruder tomountim personationandotherattacks. Tohandlesuchcriticalissues,inthis work, we design a new private blockchain-envisionedaccess control schemefor PervasiveEdge Computing (PEC) in IIoT environment, called PBACS-PECIIoT. We consider the private blockchain consisting of the transactions and registration credentials of the entities related to IIoT, because the information is strictly confidential and private. The security of PBACS-PECIIoT is significantly improved due to usage of blockchain as immutability, transparency and decentralization along with protection of various potential attacks. A meticulous comparative analysis exhibits that PBACS-PECIIoTachieves greater security and more functionality features,and requires low costs for communication and computationalas comparedto other pertinentschemes.

III. METHODOLOGIES

Theproposedprojectaimsto developablockchain-basedframework,SecPrivPreserve,to enhancethesecurity, privacy, and integrity of data in IoT-based smart city applications. As smart cities increasingly rely on IoT devices for monitoring,managing,and improvingurbanlife,ensuringsecureandefficientdatasharingamongthesedevicesbecomescrucial.Currentcentralizedsystemsarevulnerabletosecuritybreaches,datatampering,andprivacyviolations,whichcompromisestheeffectivenessofsmartcityservices.TheSecPrivPreserveframeworkaddresses these challengesby leveragingblockchaintechnologyto createa decentralizedand tamper-proofsystemfor data storage,transmission,andsharing.Itintegratesvarioussecuritymechanismssuchas OTP-basedpasswords,
encryption,hashing,andQRcode-basedencryptiontosafeguardsensitivedataandensureprivacy.
Thefollowingmodules:

- UserInterfaceDesign
- MSP
- Authority
- Client
- Upload
- SmartContract

1) UserInterfaceDesign

Toconnectwithserverusermustgivetheirusernameandpasswordthenonlytheycanabletoconnecttheserver.If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and downloadrate.Namewill beset asuserid. Loggingin isusuallyusedto entera specificpage. Itwillsearchthequery and display the query.

2) MembershipServiceProviders(MSP):

CertificateAuthorities(CA)areresponsibleforissuingX.509certificatestonetworkentities.MSPspecifieswhich CAis permittedto participatein the blockchainnetwork anduses thisinformationto identifywhichpeer nodesbelong to which groups. MSP maintains the distributed ledger between organizations and associated systems that the network trusts.

3) Authority

This is the third module in our project where Data owner has all permissionson data like delete,update,and insert on userrecordsplaysthemainpartoftheprojectrole. Authorityloginfirstthenitswithhisregistrationdataandstore his data inside cloud.

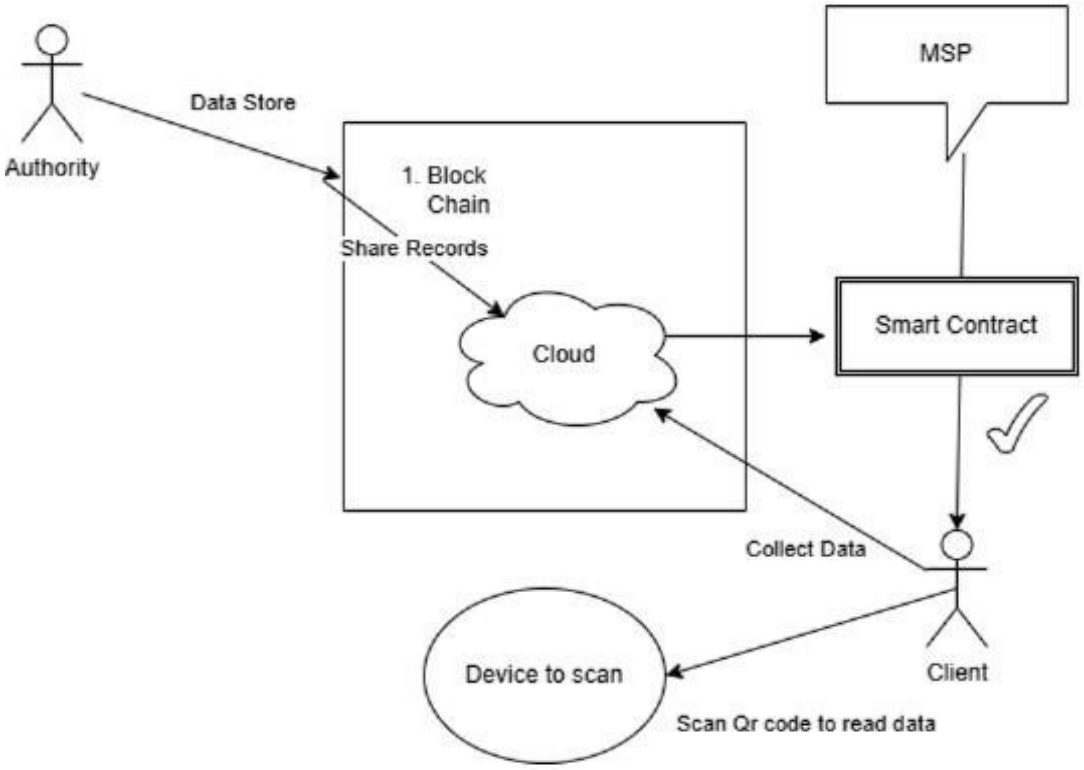
4) SmartContract

Smartcontractsaretypicallyusedtoautomatetheexecutionofanagreementsothatallparticipantscanbe immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow,triggeringthenextactionwhenpredetermineconditionsaremet.

5) Client

This is the Fifthmodule in ourproject wheredata User playsthe main part of the projectrole.User registerand then login in to the application, the registration details are stored inside database. After User Login he will directly navigate Userhome pageand Accessdata bysearchingwithkeyword. Whendataowneruploaddata thedatawillbeencrypted theencryptedkeys willbestoredinside databaseandkeyswillshredwithkeyrepository.

IV. SYSTEM ARCHITECTURE



In a blockchain network, various entities collaborate to ensure its proper functioning. The Client (C) collects user data records, while the Authority manages permissions like updating or deleting records. Membership Service Providers(MSP)issuecertificatestotrustednetworkparticipantsandmaintaintheledger. A SmartContract(SC)automates digital asset transfers and records transactions on the ledger. Endorsing Peers (EP) validate transaction proposals, and OrderingPeers(OP)organizeand addtransactionblockstotheledger.CommittingPeers(CP)validateandcommit these transactions,ensuringthe ledgeris up to date.Channelsenablecommunicationbetweenorganizationalpeers within the network.

V. TECHNIQUEUSEDORALGORITHMUSED

1) SecPrivPreserveframework

TheemergenceoftheInternetofThings(IoT),Industry5.0applicationsandassociatedserviceshavecauseda powerfultransitioninthecyberthreatlandscape.Asaresult,organisationsrequirenewwaystoproactivelymanage the risks associated with their infrastructure. In response, a significant amount of research has focused on developing efficient*CyberThreatIntelligence*(CTI)sharing.However,inmanycases,CTIcontainssensitiveinformationthathasthepotentialtoleakvalu ableinformationorcausereputationaldamagetothesharingorganisation.

Whilea number of existing CTI sharing approaches have utilised blockchain to facilitate privacy, it can be highlighted that a comprehensiveapproachthat enablesdynamictrust-baseddecision-making,facilitatesdecentralisedtrust evaluation and provides CTI producers with highly granular sharing of CTI is lacking. Subsequently, in this paper, we propose a blockchain-basedCTIsharingframework,called *Priv-Share*,asa promisingsolutiontowardsthis challenge.In particular,we highlight that the integrationof *differential sharing, trustlessdelegation,democraticgroupmanagers*and *incentives* aspartof *Priv-Share* ensuresthatitcan satisfythesecriteria.Theresultsofananalyticalevaluationoftheproposedframeworkusingbothqueuingand game theory demonstrate its ability to provide scalable CTI sharing in a trustless manner. Moreover, a quantitative evaluationofanEthereumproof-of-conceptprototypedemonstratesthatapplyingtheproposedframeworkwithin real-world contexts is feasible.

2) Block Chain

Blockchainis asharedimmutableledger that facilitatesthe process of recordingtransactionsand tracking assetsacrossa business network. Anythingof value can be tracked and traded on the Blockchain network. A Blockchain is a distributeddatabase,whichissharedoveracomputernetwork.Blockchainstoresinformationelectronicallyina digital format to make transactions secure.

Blockchainisanewtechnology,whichisknownasDistributedLedgerTechnology(DLT).Withthehelpof Blockchain technology, currency as well as anything can be converted into digital format and stored. Actually it is an exchangeprocess,whichworkson datablocks.In this,oneblockisconnectedtoanotherblock.Theseblockscannot behacked.Blockchaintechnologyaimstokeepdocumentsdigitallysecure.YoucantakeGoogleDocasanexampletounderstandBlockchaintechnology.Whenwecreatea documentandshareitwithagroupofpeople,thedocument is distributedinstead of copiedor transferred.But, Blockchainis more complexthan Google Doc. Simply put, Blockchainis known as DistributedLedger Technology, which makes any digital asset immutableand transparent through the use of decentralization.

3) Smart Contract

A smart contract is a self-executing program that automates the actions required in a blockchain transaction. Once completed, the transactions are trackable and irreversible. The best way to envision a smart contract is to think of a vending machine—when you insert the correct amount of money and push an item's button, the program (the smart contract)activates the machineto dispenseyour chosen item.

Smart contractspermit trustedtransactionsand agreementsto be carried out among disparate,anonymousparties without the needforacentralauthority,legalsystem,orexternalenforcementmechanism.

Whileblockchain technologyhascome to bethoughtof primarilyas thefoundationfor Bitcoin,it has evolvedfar beyond underpinning a virtual currency.

VI. CONCLUSION

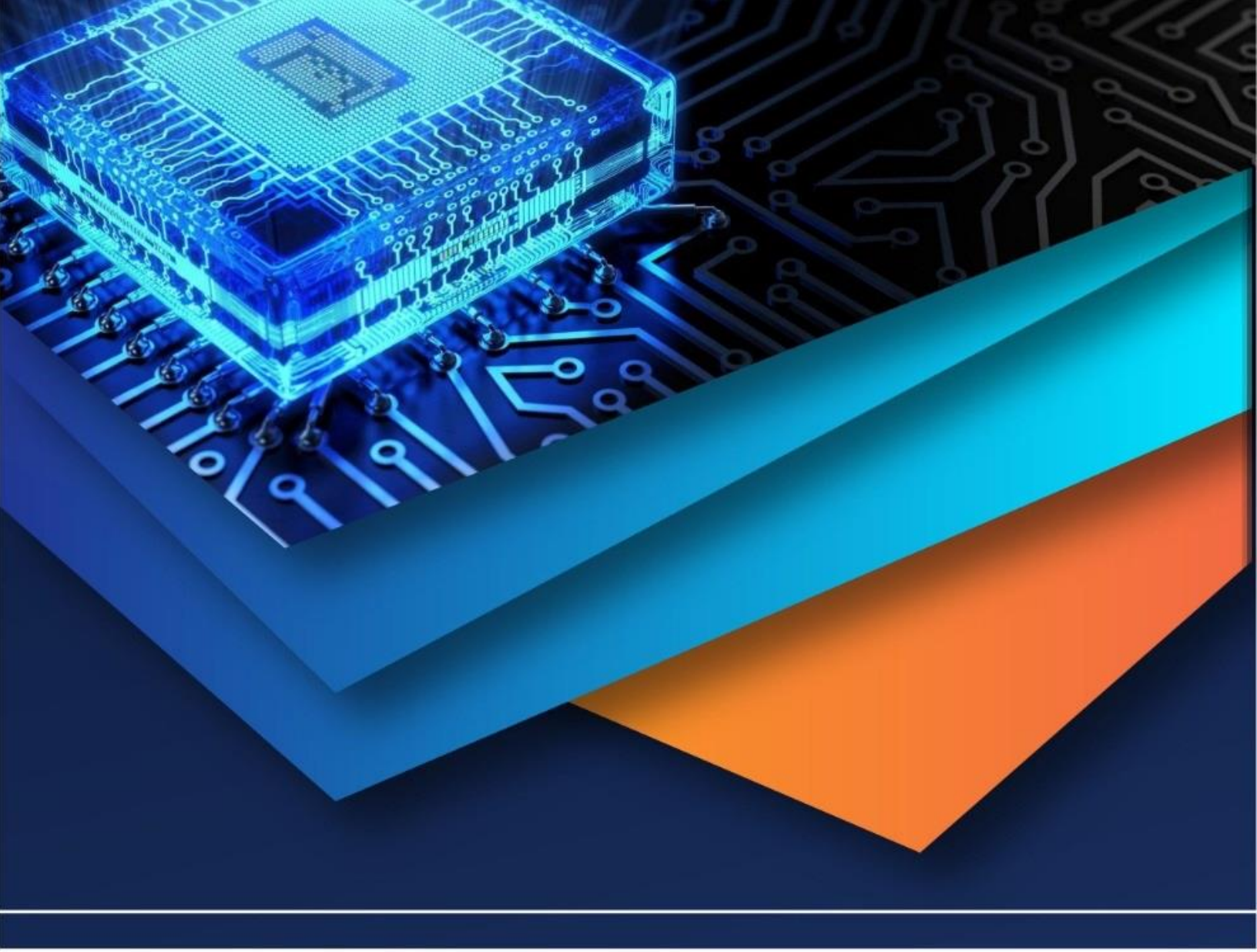
In this paper, Blockchain secures and anonymizes IoT and its applications. Smart city challenges include user security, privacy, bandwidth, anonymity, and scalability. Therefore, this study proposes a blockchain-based SecPrivPreserve system. The presented framework ensures the privacy and safety of the user's data throughout processing. In the Hyperledger Fabric blockchain, information is summarized, and specific features of business transmission are systematized based on the model. Initialization, registration, data protection, authentication, data access control, validation, data sharing and download comprise in SecPrivPreserve framework.Security features include passwords, OTP, encryption, hashing, digital signature, Chebyshev polynomials, and interpolation. Cutting-edge experiments demonstratedthatSecPrivPreserveoutperformedstate-of-the-artsystemsinresponsiveness,processingtime, encryption quality, and detection rate. However, the experimentation was carried out through Fabric SDK, and the obtainedresultsshowthattheproposedframeworkreducescomputationaltimeandresponsiveness

REFERENCES

[1] C.Vanmathi, R. Mangayarkarasi,and R.J. Subalakshmi, ''Real timeweather monitoringusing Internetof Things,'' inProc.Int.Conf.Emerg. TrendsInf. Technol.Eng.(ic-ETITE),Feb.2020,pp.1–6.
[2] B.BryantandH.Saiedian,''KeychallengesinsecurityofIoTdevicesandsecuringthemwiththeblockchain technology,'' Secur. Privacy, vol. 5, no. 5, p. e251, Sep. 2022.
[3] F.Al-Turjman,H.Zahmatkesh,andR.Shahroze,''Anoverviewofsecurityandprivacyinsmartcities'IoT communications,'' Trans.Emerg. Telecommun. Technol., vol.33,no.3,p.e3677,Mar.2022.
[4] TheEditorsofEncyclopaedia.(Dec.9,2023).UnitedNationsPopulationFund.EncyclopediaBritannica. Accessed: Jun. 6, 2023.

[5] V. Moustaka,Z. Theodosiou,A. Vakali, and A. Kounoudes,‘‘Smartcitiesatrisk!Privacyandsecurityborderlines fromsocialnetworkingincities,’’ inProc.Companion TheWebConf.WebConf.,2018,pp.905–910.
[6] I.Makhdoom,M.Abolhasan,J.Lipman,R.P.Liu,andW.Ni,‘‘AnatomyofthreatstotheInternetofThings,’’ IEEECommun.SurveysTuts.,vol.21,no.2,pp.1636–1675,2nd Quart.,2019.
[7] K.Zhang,J.Ni,K.Yang,X.Liang,J.Ren,andX.S.Shen,‘‘Securityandprivacyinsmartcityapplications: Challengesandsolutions,’’ IEEE Commun.Mag. ,vol.55,no.1, pp.122–129,Jan.2017.
[8] S. Chaudharyand P. K. Mishra,‘‘DDoS attacksin industrialIoT: A survey,’’Comput.Netw., vol. 236,Nov.2023, Art. no. 110015.
[9] L.Cui, G. Xie, Y. Qu,L.Gao,and Y. Yang,‘‘Security and privacy in smart cities: Challenges and opportunities,’’ IEEE Access, vol. 6, pp. 46134–46145, 2018.
[10] Z.XihuaandD. S.B. Goyal,‘‘SecurityandprivacychallengesusingIoTblockchaintechnologyina smartcity: Criticalanalysis,’’ Int.J.Electr. Electron.Res.,vol.10,no.2,pp.190–195,Jun.2022.
[11] P. M.RaoandB. D.Deebak,‘‘Securityandprivacyissuesinsmartcities/industries:Technologies,applications, andchallenges,’’ J.AmbientIntel l.Humanized Comput.,vol.14,no.1,pp.1–37,Feb.2022.
[12] M. Ramaiah,V. Chandrasekaran,V. Ravi,and N.Kumar,‘‘An intrusiondetectionsystem usingoptimizeddeep neuralnetworkarchitecture,’’ Trans.Emerg. Telecommun.Technol.,vol.32,no.4,p.e4221, Apr.2021.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)