e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:05/Conference:01/March-2023 Impact Factor- 7.868 www.irjmets.com

National Conference on Trending Technology for Achieving Sustainable Development Goals

NCTTASDG 2023 Organized by Shri Shankarprasad Agnihotri College of Engineering, Wardha

BLOCK CHAIN BASED IDENTITY VERIFICATION SYSTEM

Prof. N. B Vairagde[*1], Avinash Waghmare[*2], Nilesh Deshmukh[*3], Prajkta Thool[*4], Mayur Darunde[*5], Sunil Wete[*6], Prof. C. D. Sawarkar[*7], Prof. M. A. Ramteke[*8]

[*1,7,8]Prof. Department of Computer science & Engineering SSPACE, Wardha Maharashtra, India

[*2,3,4,5,6]Student, Department of computer science &Engineering SSPACE, Wardha ,Maharashtra, India

ABSTRACT

ItisbasedonCybersecuritydatasetCloudserviceshaveincreasedthenumberofdataownersithasbeenstoretheirencryptеddatainthecloud,whileanequalorgreaternumberofdatausersbasedindataretrieval.ItisbasedonBlockchainHybridECCandAESAlgorithmusingtheEncryptedandDecryptedthedataset. Encrypted File will be Stored in Cloud ServerandUserbasedonKeywordSearchingforAlgorithm.UserbasedEnterthekeywordthatalsoEncryptedQueryAfterthatSearchingEncryptedCloudServerFinallyRetrievaltheRelatedFileonQuerybased.UserbasedentertheParticularkeyuserdecryptsFilethebetterperformancebetterperformanceintermsofrecall,rankingprivacy, precision,searchingtime

Keywords: Blockchain, Self-sovereignIdentity,authenticationmechanism,Identifyproofing,claimverification.

I. INTRODUCTION

- Identitytheftistheunauthorizedacquisitionofanotherperson'sconfidentialinformationinordertomisuseit.
- Inanyregistrationprocesswehavetobringphysicaldocumentthatcausesunauthorizedaccessofuserspersonaldocument.
- ABLOCKCHAINTECHNOLOGYcansolvethisproblem.
- Inthis,asystemcalledBlockchain-basedpersonalIdentitysecuritySystemisproposedwherebyitisasystemwhichstoresanindividual'spersonal recordsonthe blockchain.
- Thissystemusesthesecurityfeaturesofblockchaintoalloweveryonetoknowwhohasaccessto theirdata

II. METHODOLOGY

In this research, our motivation is to develop a concept that maximizes the transparency as well as the controloverpersonaldataforusers.MyDatahasproposedahuman-centricapproachthatempowerstheuserbyplacinghimin thecenter ofhisdataecosystem.

Themainfocushereisnotowningthedata(i.e.storingthedataontheuser'sownserver),buttocontrolthedataflowfrom datatoserviceproviderbycontrollingtheassociatedconsentsfromtheusertotherespectiveservice.While the approach of My Data, requires a significant shift in the ecosystem and that service providers agree onthis way of handling data, we sought to develop an approach that can enable a fair balance in the ecosystemwithoutsupportfromtheserviceprovider,but onlythroughtechnologyandlegislativemeans.

III. MODELINGANDANALYSIS

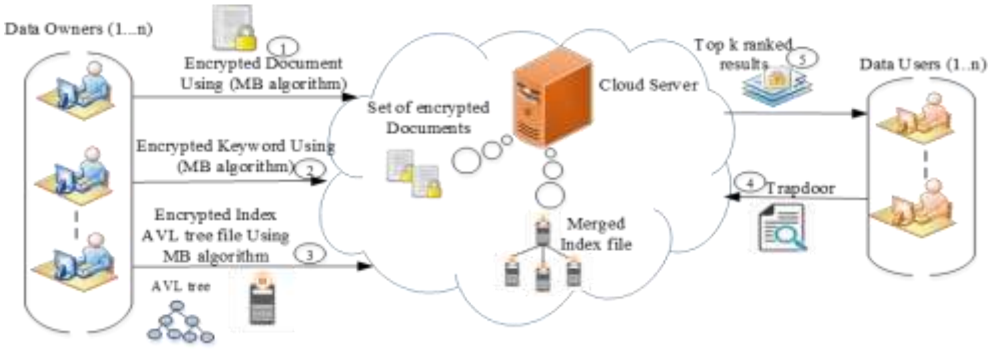

Data Owners (1...n)
1
Encrypted Document Using (MB algorithm)
Encrypted Keyword Using (MB algorithm)
2
Encrypted Index AVL tree file Using MB algorithm
3
AVL tree
Set of encrypted Documents
Cloud Server
Merged Index file
Top k ranked results
5
Data Users (1...n)
4
Trapdoor

Figure1: Architecture

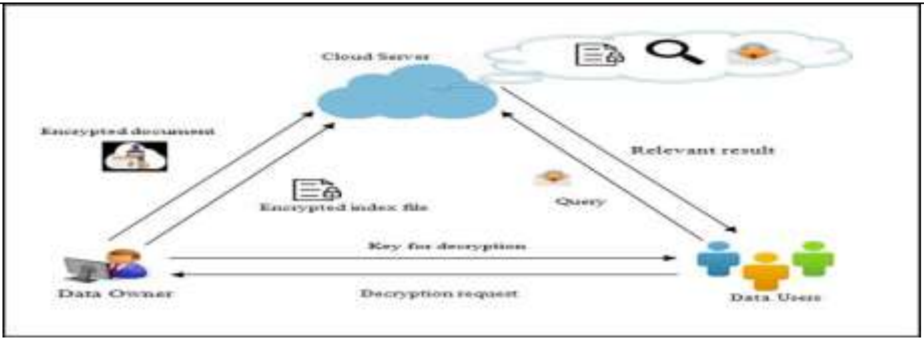


Figure2: BlockchainBasedIdentityVerificationSystem

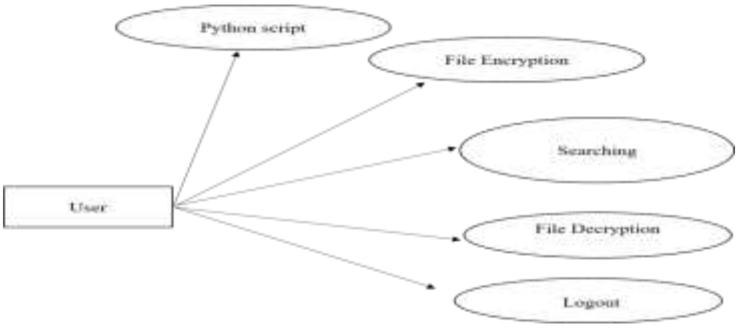


Figure3: UseCaseDiagram

- Auserwants toaccessaservice,whichtheproviderrequestsinformationfor
- Theuserauthenticateshimselfto the personaldatastoragethroughhisprivatekey
- A consent transaction is created on the blockchain with a shared identity of the service provider andtheuser.This gives theprovideraccesstothatdata point aswellas the identityblockchain
- The service provider can read run the information through the stored hash and verify the informationtheuser has successfullyidentifiedhimself andthe providerhasonlythe informationneeded.

IV. DATASELECTION

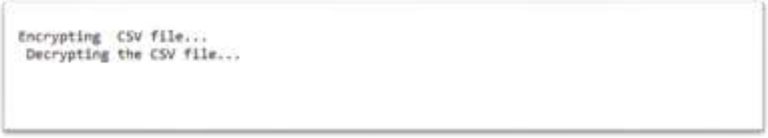
- Cybersecurityistheuseoftechnologies,processes,andcontrolstodefendagainstcyber-attacksonsystems,networks,programs,devices,anddata.
- Itsgoalistoreducetheriskofcyber-attacksandtoprotectagainstunauthorizeduse ofsystems,networks,andtechnologies.
- CybersecurityProtocolsReferenceandKeywords
- Inthisstep,wehavetoloadthedatawiththehelpofpanda’spackages

V. DATAPREPROCESSING

- Datapre-processingistheprocessofremovingtheunwanteddatafromthedataset.
- Prerocessingdatatransformationoperationsareusedtotransformthedatasetintoastructuresuitableformachinelearning.
- Missingdataremoval:Inthisprocess,thenullvaluessuchasmissingvaluesandNanvaluesarereplacedby0.
- asvariableswithafinitesetoflabelEncodingCategoricaldata:Thatcategoricaldataisdefinedvalues.

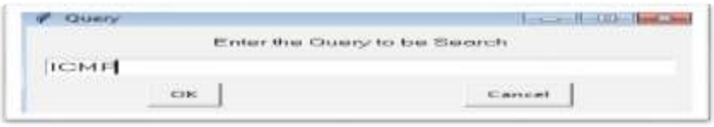
VI. HYBRID ECCAND AESALGORITHM

- ECCElliptic CurveCryptograph AlgorithmbasedonPublic andPrivateKey
- ECCand AESbasedonEncrypted data
- ThequickexplanationisthatkeysusingEllipticCurveCryptography(ECC)areasymmetric(publicandprivate),whereasAES-256usesasymmetric cypher(key)
- ECCand AESbased onitPublicand Privatekey



```
Encrypting  CSV file...
 Decrypting the CSV file...
```

- HybridAESandECCbasedon **128 bitkey** GeneratedForEncrypteddataWise



Query

Enter the Query to be Search

ICMR

VII. Key Generation

- HybridAESand ECCbasedon128bitkeyGeneratedForEncrypteddataWise
- Aencryption systemisdesigned bycombiningthecharacteristicsoftheAESand ECC
- WhichCansolveSecurityProblemitself
- Efficientlyrealizetheinformation,dataencryption,signature,andidentityverification

VIII. Cloud Me

- EncryptedFileWillbeStored indataforSecuritypurpose

  AcloudcomputingmodelinwhichdataisstoredontheInternetviaacloudcomputingproviderwho managesand operatesdata storage asa service CloudServer willbeusedonCloudme Software

IX. RESULTSANDDISCUSSION

Regardingthetestingwhichispartofthetransitionphase,thereweretwotypesoftestingdone:systemandacceptancetesting.ThesummaryoftestcasesisinTable2,wherebytherewereatotalof18casesforeachofthefunctionalitiesinthe web application as well as the Android application. The functionalities are as follows: authority, requester and userregistration,authorityand userlogin,uploaduser details, andrequestuserdetails.

X. CONCLUSION

HybridECCand AESAlgorithmusingtheEncryptedandDecryptedthedataset

Encrypted File will be Stored in Cloud Server and User based on Semantic Searching method Algorithm.UserbasedkeywordEnteringisdonetoretrievethecorrespondingdatafilefromthecloudstorage.

FinallyRetrievetheRelatedFilebasedonQuery.ThiswilleasilyFindout**CybersecurityProblem**like,thefaultfilewillbedetected

XI. REFERENCES

[1] Pascual, A., Marchini, K., & Miller, S. (2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity.Retrievedfromhttps://www.javelinstrategy.com/coverage-area/2018-identityfraudfraud-enters-new-era-complexity

[2] O.N.GuyZyskindandA.S.Pentland.(2015)DecentralizingPrivacy:UsingBlockchaintoProtectPersonalData https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013169

[3] https://academicjournals.org/journal/JLCR/article-full-textpdf/8599A6F7684

[4] https://www.researchgate.net/publication/222808883_Biometricbased_personal_identityauthentication_system_and_security_analysis

[5] Yasin, A., & Liu, L. (2016). An Online Identity and Smart Contract Management System. In 2016 IEEE 40thAnnual Computer Software and Applications Conference (COMPSAC). Atlanta, GA: IEEE. Retrieved fromhttps://ieeexplore.ieee.org/document/7552202