A Framework Of Big Data As Service Platform For Access Control & Privacy Protection Using Blockchain Network

Santosh Kumar Sharma[1*], Ajay Pratap[2] And Harsh Dev[3]
1, 2 Amity Institute Of Information Technology, Amity University, Lucknow
3 Dept. Of Computer Science & Engineering, Pranveer Singh Institute Of Technology, Kanpur

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract
Big Data As A Service Is Used In Today's Scenario To Handle And Process The Big Amount Of Data Which Are Generated From Different Source Every Day. Since Data Is Stored On The Cloud Platform, The System Could Suffer A Failure And Give Attackers The Opportunity To Launch Various Categories Of Attacks.Manyresearcheshave Been Done In This Domain To Provide Security And Protection To The Data On Cloud. The Blockchain Technology Is A Secure, Distributed And Privacy-Preserving Decentralized Ledger Where The Transactions Are Flexible, Secure,Verifiable And Permanent Way.Here, The Transaction Data Is Encrypted Andkept In A Wrapped Block (I.E., Record) Which Are Spreadthrough The N/W In A Provable And Unabashedmode Across The Entire Network To Enhance Information Security And Data Privacy. In This Paperwe Have Proposed A Framework For An Access Control With Privacy Protection In Bdaas Based On Blockchain Technology. Here Blockchain Technology Is Used Only For Storing The Transaction Log Information Whenever Any Kind Of Event Log Occurred In System.

Keywords: Big Data As A Service, Blockchain, Privacy, Access Control

Introduction

As We Know That In Today's Scenario Data Is Very Important And Key Assets For Any Organization Since Many Times Decision Are Based On These Data. Data Is Generated From Dissimilar Sources Like Sensor Data, Social Networking Sites Data (Facebook, Twitter, Whatsapp, Etc.), Educational Data, And Government Data And So On. These Kinds Of Data Can Be Structured, Semi Structured And Unstructured In Nature. To Handle And Process Such Kind Of Huge Data A New Concept Big Data As A Service (Bdaas) Was Presented In [1],Which Is A New Conceptual Model That Combines The Storing And Computationabilities Of Cloud Computing With Processing Power Of Big Data For Delivering Data, Database, Data Analysis, And Processing Platform Services, Along With Traditional Service Models (Paas, Saas And Iaas). Bdaas Is A Cloud-Based Framework For Delivering The Point-To-Point Big Data Solutions To The Business Organizations On The Requirement Basis. It Is Also Defined As Combined Capabilities Of Data As A Service (Daas), Hadoop As A Service (Haas) And Data Analytics As A Service (Daaas). It Includes Different Service Models To Fulfill The Specific Demands Of Big Data Systems. A Bdaas Cloud Infrastructure Must Offer Functionalities As Big Data Storage, Computing, Data, Databaseandanalytics Software As A Service [1].

Although There Are A Lot Of Benefits Of Using Bdaas But At The Same Time Access Controland Privacy Of The Data Become Very Important And Critical Issue When Data Is In Rest, In Motion Or In Process Since Data Is Kept On Cloud Storage Which Are Scattered. According To The Published Report Of Cloud Security Alliance In 2017, Access Control Is One Of The Most Critical Security Issues [12]. Researchers Have Developed Various Methods For The Access Control And Privacy Of Data But Still There Is A Need To Analyzeit Such As Data Violation, Data Exposure, And Malicious Activities Done By Cloud Users [2][3].

Therefore, Cloud Service Providers Do Not Assure About What Levels And Type Of Protection Are Needed For Suitable Big Data Security And Privacy. It Means That The Previously Mentioned Issues Which Are Related To Access Control And Privacy Of The User's Data Must Be Taken Into The Process In Adoption Of Cloud Computing Services.

In The Recent Years, The Blockchain Technology Can Be A Good Solution Which Has Introduced On The Market To Prove A Secure Decentralized Atmosphere For Information Sharing [4][5]. Blockchain Was Primarily Designed For Exchanging Crypto Currency As Its Basic And Primary Technology, But It Can Be Used In Other Application Areas For Providing Security And Privacy To The Datafor Example Educational Systems [9], Internet Of Things (Iots) [6], Smart City [8], Smart Home [7], And Healthcare [10]. Bitcoin Is The First And Most Popular Application Of The Numerousupcoming Blockchain Operations In Real World Applications. Technically, Blockchain Is A Scattered And Decentralized Community Ledger (Record) That Holds Whole Transactions Grouped In Blocks That Ever Completed In The N/W. The Blockchain Technology Works On Point-To-Point (P2p)N/W Where Each Node Keeps A Copy Of The Blockchain Record. In This System There Is No Central Regularity Authority To Manage The Blockchain Databases. Blockchain Technology Ensures The Protection Of The Data Kept In Blockchain Database And Keeps Safe From The Security Attacks.In This Paper We Have Proposed A Framework For Access Control& Data Protection In Bdaas Based On Blockchain Technology For The Purpose Of Providing The Access Control And Data Protection To The Users Who Need Data Storage, Processing, Computing, Analytics, Etc. As A Service From Big Data As A Service Platform.

The Rest Of Paper Is Organized As Follows. In The Next Section, We Have Briefly Described The Background Of Bdaas Technology And Blockchain Technology Followed By The Proposed Bdaas Framework Based On Blockchain N/W. Then, We Have Discussed The Security And Privacy Significances Of The Proposed Framework. And Finallyat The Last, We Have Conclude Our Work.

Big Data As A Service (Bdaas)

Bdaas Is A New Direction To Get Valuable And Clear Perception From Big Data. It Is Also A New Class Of Service Type. By Enclosingdiverse Data As A Service, It Covers The Variations On Data Structure And Descriptions, And The Users Only Concern About Their Need And Get The Service Whenever And Wherever They Want To Store The Data, Analyze The Data And Visualize The Data [11]. It Offers Users Popular Big Data-Related Services To Improve Productivity And Minimize Costs.Itprovides Different Levels Of Abstractions To The Users Andtypically Includes Three Layers As Big Data Infrastructure As A Service (Storage As A Service And Computing As A Service), Big Data Platform As A Service (Data As A Service And Database As A Service) And Big Data Analytics Software As A Service [1]. Big Data As A Service Platformoffers A Lot Of Benefits Such As Cost Reduction, Better And Fast Decision Making, Better Data Visualization, Better Quality, Quick Response, Data Management And Data Analytics. In Today's Scenario Multiple Companies Likeibm, Emc, Amazon, Microsoft, Google, Oracle, Sap, Snaplogic, Etc., Have Occupied Big Data As A Service Market Space And Provide Mainly Big Data Storage And Analysis Service. For Example, Emc Offer Services For Big Data Storage And Data Analysis. Greenplum Is A Tool Set Of Emc For Data Storage And Analysis, Provide Storages Services And Allows User To Use The Services Of Hadoop For Bda. Amazon Provides Independent Bda Services Though Amazon Work Space Marketplace. Through Windows Azure Marketplace, Microsoft Provides Bda Services. Google Provides Bda Services Through Google Bigquery.

Since Bdaas Is A Cloud-Based Service Platform And Data Is Distributed On Different Servers, Users Are Very Much Concern About The Security And Privacy Of Their Data. Also Cloud Computing Suffers From Multiple Kind Of Security Issueslike Data Theft, Data Manipulations, Data Loss, Denial Of Service, And Suspicious Or Malicious Insiders Mostlygenerated From Issues Such As Multi-Tenancy, Loss Of Control And Trust Over Data [12] [13]. Therefore, The Levels Of Data Security And Access Control Do Not Ensured By Most Of The Cloud Service Providers In Their Slas As Part Of The Prescribed Terms And Conditions B/W Service Providers And Customers. Therefore,It Is Necessary To Think Over The Term Securityof Data And Access Controlwhile Using Big Data As A Service By All Parties Involved In It.

Blockchain Technology

The Blockchain Is New And One Of The Rising Technologies That Have Grown Quickly In Current Years, And Bitcoin Is Its Highly Successful Application Of It [14]. It Is Decentralized And Distributed By Nature. Blockchain Is A Defined As P2p (Pear To Pear) Distributed Database (Ledger), Used To Maintain A List Of Regularly Growing Transaction Records (Known As Blocks). These Blocks Are Linked To Each Other And Normally Public Key Cryptography (Pkc) Is Used To Provide Security In Blocks [4]. Formally, A Blockchain Is Considered As A Combination Of Two Parts As Blocks Or Storage Units (Used To Store Transaction Records That Ever Completed In The System) And Chain Or The Connection Links Of All Time-Stamped Transaction Records Into Continuous Chain Network [15]. Unlike Centralized System, In Blockchain N/Wnoveldata Or Transaction Is Insertedinto The Blocks And These Are Distributed To All The Nodes Participated In That Distribute System. Each And Every Block In This System Is Denoted Through A Hash Value (Securely Created) Using Sha256 Which Is The Secure Hash Cryptographic Algorithm[4]. In This Mechanism The Present Block (Parent) Is Connectedwith The Subsequent Continuous Block (Child) And Hash Value Of Parent Is Stored In The Child Block As In Figure 1. In This Way If The Contents Of Any Block Are Changed Then Secure Hash Value Will Also Be Modified With It And It Will Be Broadcasted To The Wholen/W To Nullifythe Block. A Private Key Is Assigned To Each And Every Participant Of The Blockchain Network For Signing(Digitally) And Validating The Transaction They Make.

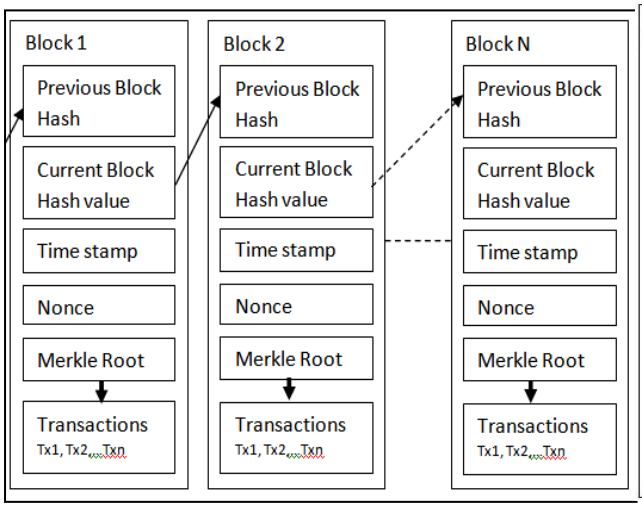

Figure 1: Basic Structure Of Blocks

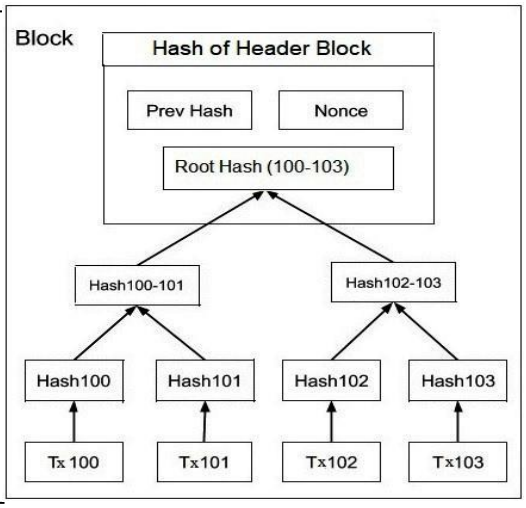

Figure2: Merkle Tree

As In Figure 1 A Block Contains Header And Long List Of Transactions. Block Header Generally Contains Timestamp Value (Denote The Time Of Block Creation), A Nonce Randomly Generated By Consensus Algorithm For Computing Block's Hash Value, Block Version Number And Pod Which Is A Securely Created Hash Value That Shouldbe Always Fewer Than The Present Hash Value Of The Block. For Summarizing All The Transactions Within A Block, Blockchain Technology Uses A Merkle Tree As In Figure 2. Here All The Transactions Are Connected Together Using This Tree [4]. For Validating The Transactions, All Nodes In This Network Use And Run Consensus Algorithm [16][17]. In Consensus Algorithm Pow, The Miner Nodes Need To Solve A Difficult Mathematical Puzzle If A New Block Needs To Be Added In This Network. This Process Requires Great Computational Power.

In Consensus Algorithm Pos, Pseudo-Random Voting Method Is Used To Choosea Node To Be The Validator Of The Subsequent Block Depending On Its Wealth [17]. In This Algorithm No Need To Solve The Accurate Puzzle, Only The Wealth Of Validator Is Needed For Validating The Transaction And Block. Dpos Is An Extension Of Proof Of Stake(Pos) Algorithm That Is Maintained By An Election System For Choosing Nodes (Called Witnesses) For Verifying The Blocks. It Is The Responsibility Of The Witnesses To Make And Add Blocks To The Blockchain N/W, Also To Limitmischievous And Dangerous Nodes From Contributingin The Task Of Additionthe Blocks In The N/W.

Blockchain Network Can Be Categorized As Private, Public And Consortiumchain [17], [18]. The Public Chain (Also Known As Permissioned Less Chain) Is Entirely Decentralized N/W Where Any Node Of Thisn/W Can Contribute In The Writing, Reading, Verification, And Consensus Processes Of The Records On The Chain. The Private Chain (Also Known As Permissioned Chain) Is A Centralized Blockchain. Where The Access Permission Of The Records On The Chain Is Regulated By The Central Or Chief Authority, And Only The Restricted Nodes Are Allowed To Join The Network. The Consortium Chain (Mixture Chain) Is A Partly Distributed Blockchain Where Previously Electednodes Jointly Determine The Generation Of Each Block. Other Nodes Of The N/W Can Have The Rights To Access The Blockchain For Transactions, But They Are Not Authorized Participate In The Consensus Process.

Review Of Literatures

Literature Reviews Reflects That At First Bdaas Was Proposed In [1], Where The Authors Simply Presented The Threeservice Layers As Big Data Analytics As A Service, Big Data Platform As A Service And Big Data Infrastructure As Aservice Without Giving The Details About How To Design And Provide The Services To The Cloud And Also Security Aspectis Also Missing. Another Framework Was Introduced In [19] Where All The Aspects Of The Big Data Life Cycle(Acquisition, Storage, Processing And Visualization) Were Missing.

Another Framework Was Introduced In [20] Where All Aspects Of Big Data Lifecycle Was Defined But Security Aspectwas Missing. A Lot Of Researches Have Been Done In The Direction Of Providing The Security Of The Data In The Cloud-Based Scenario.

In [21] The Author Has Proposed An Accesscontrol Algorithm Forbig Data Cloud Tomaintain The Privacyof User Using Role-Based Access Controlprototype,Symmetric Encryption,Andciphertext Attribute-Basedencryption. In This Paper Privacy Of User's Data Is Achieved Alongwith Access Control But It Is Limited To Only Smalldata Size Which Needs To Be

Extended For Bigger Sizedatasets In Future. In [22] An Encryption(Attribute-Based) Waspproposed By Theauthors To Maintainthe Privacy Using Secure Hash Algorithm, Symmetric Key Approach And Pailier Algorithm. Here, Anonymousauthentication Isachieved Which Providesuser Revocation Andprevent Replay Attacks But Protection Of The Data In The

Cloud May Be Compromisedsince Access Policy For Eachrecord Is Known To The Cloud. Another Privacy Preserving Approach For Cloud Computing Was Proposed In [23] Using Paillier Encryption Algorithm, Elliptic Curve Encryption Algorithm Andeigen-Face Encoding Algorithm. This System Takes More Time Duringmatching Facial Encryptionand Image Data, Also It Failswhen Database Is Very Small.It Needs Further Improvementto Develop Automaticbiometrics-Basedauthentication System. In [24] A Novel And Productive System Was Proposed For Sharing Information In Cloud Computing Environment Using Abe Algorithm,Distributed Hash Tablen/W, Identity-Based-Time Release Encryption Algorithm. Although, This System Provides The Security Against Various Attacks But There Is A Problem In It That Users Have To Depend Uponthe Data Owner For Assess. In [25] Another Scheme 1024-Bit Dna Based Encryption Was Proposed For Providing Data Security In Cloud Computing Environment. Experimental Findingsindicate That This Methodis More Successful Thanother Existing Systemsand Produces Betterresults Than Others But Still Improvements Are Needed. In [26] A Novel Concept Cp-Abealong Witheffective Authoritytest Was Proposed Forpreserving Theprivacy And Enhancing The Access Control. There Are So Many Advantages In This Scheme But Still It Suffers From A Restriction That It Only Supports "And" Strategy And Depend On A Weak Security Model.

In [27] Block Chain Based Frame Work For E-Governance Was Proposed To Provide Privacy And Access Control Using Digital Signature And Encryption Techniques. Only High-Level Concepts Are Proposed And Needs To Discover Its Full Potential. In [28] Authors Have Designed A Social Media Network: *Ushare,*

Based On Block Chain Using Turing Complete Relationship System, Blockchain, A Hash Table With Encrypted Content A Local Personal Certification Authority
(Pca). This System Was Also A Framework Only And Needs To Be Further Mathematically Valuated. In [29] A Framework For Bigdata Securitysharing Wasdesigned Based Onblockchain Technology And Smart Contract. This Model Provides The Solution Forthe Architectural Securityand Protection Againstforged Block Attack But The Drawback Is Every Node Needs Morestorage And Computingpower For Storing Data In The Blockchain Which Needs To
Be Further Investigated. In [30] Asecure Distributed Vehicular Network Architecture Is Proposed For Smart Cities Based On Block Chain And Smart Contract. Theauthors Have Proposed A Trust Management System Where Blockchain Stores The Trust Value Of The Nodes, Used To Determine The Authenticity Of The Nodes Which Are Involved In The Network. This System Is More Efficient To Share The Information In Vehicular Network But There Is An Issue Related To The Cost Of The System Which Can Be Increases When Data Size Will Be Increases. In [31] An Access Controlecosystem Using Blockchain Networkwas Proposed Forbig Data Security Using Identity Based Accesscontrol, Hyperledger Fabricblockchain Androle Based Access Control. The Proposed System Isauditable, Highly Secureand Flexible Enough Tofor Big Data Security But There Is One Challenge That It Is New Concept Which Suffers From The Proper Stability.
In [32] The Authors Have Given An Analysis Report On Privacy-Preserving Techniques For Big Data Analysis In Cloud Platform. In This Paper They Also Compare The Different Privacy Preserving Techniques. In [33] Authors Have Proposed Micro Blockchain Based Intrusion Detection System To Configure Ids Dynamically Based On Their Location Dissimilarity. Another Framework Bpay (A Payment System)Of Cloud Computing Outsourcing Services Was Introduced In [34], Which Was Based On The Blockchain Technology. Also,It Was Best Suited With Bitcoin And Ethereumblockchain. In [35] Distributed Security Architecture Of Cloud Storage Was Proposed Where Before Uploading The Files Were Partitionedinto Blocks Of Data Which Were Encrypted, And Then The File Copy Placement Problemwas Solved Using Genetic Algorithm. In [36] A Blockchain Based Cloud Database Design Was Proposed To Guarantee The Integrity And Reliability Problem In Cloud Environment. In [37] Blockds Was Proposed Which Is A Securetechnique Of Distributed Records Storage And Keyword Search Facility To Resolve The Conventional Trust On A Reliablenode In Cloud Storage System. In [38],The Issues Of Reliability Of Data Sources In Cloud System Was Resolved Throughblockchain Consensus Algorithms. In [39] A Cloud Data Deletion Protocol Was Introduced For Solving The Behavior Of Corrupt Users By Altering With Data Removaloutcomes When Cloud Server Is Not Reliable. In [40] A Cloud Forensics Scheme Was Proposed Which Is The Combination Of Blockchain And Cryptographic Signature Techniques.

Proposed Framework

As We Have Discussed In The Previous Section, A Lot Of Research Have Been Done In The Area Of Providing Security To The Data In Cloud Computing. Also, A Lot Research Has Been Done To Secure The Data In Big Data. But Still There Is A Requirement To Work On Analyzing The Security Requirements In Big Data As A Service Platform. Many Researchers Have Proposed Better Solutions For The Access Control In Cloud Computing Or Big Data But No One Has Extended Their Solution For The Bdaas Platform. Therefore, We Have Proposed A Framework For Access Control In Bdaas To Provide Data Security Using Blockchain As Tool. Previously Framework And Architecture Of Bdaas Were Already Proposed In [1], [11], [19], [20] But Security Aspect Was Not Properly Analyzed In These Frameworks. As We Know That Blockchain Network Is Most Secure Network Till Now. Our Proposed Framework Is Illustrated In Following Figure 3.

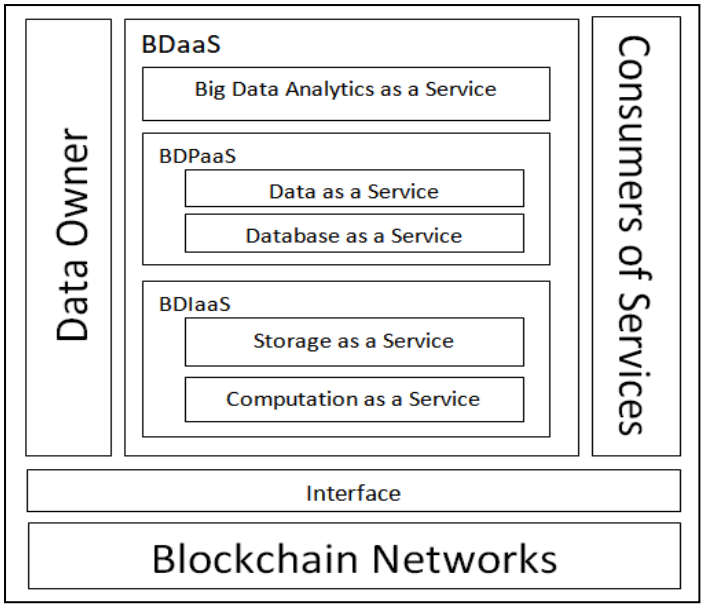

Fig3: Proposed Block Chain Based Bdaas Framework

As Shown In Figure 3 Our Proposed Framework Has Four Components As Data Owner Or Producer, Bdaas Platform, Block Chain Network And The Consumers Of The Services. Data Owner Or Data Producer Can Be Any Source From Where Data Is Produced Such As Sensor Network Data, Educational Data, Social Network Data, Research Institutional Data, Enterprise Data, Government Data, And So On. Such Kind Of Huge Data Is Collected In Massive Form And Can Be Organized, Semi Organized And Unorganized In Nature. Bdaas Platform Provides The Different Kind Of Services Like Analytics Services, Storage Services, Computation Services, And So On. A Blockchain Network Ensures The Data Security And Access Control During The Processes In The Network. And The Consumers Of The Services Can Be Any Different Kind Of Individuals Including A Single Person Or An Organization. Consumers May Initiate A Transaction Request Of Service, That Requests The Data Producer Or Service Producer To Supplydata Or Service Usage Privilegesthrough Blockchain And Obtain An Approved Data Set Or Service.

All Components Of This Framework Must Register To The Blockchain N/W. Data Owner Or Producer Of The Data Must Register On The Blockchain Network Before Uploading The Data On The Cloud Based Bdaas. Big Data As A Service Register On The Blockchain Network To Ensure The Security And Privacy Of The User's Data. Consumers Of The Services Also Register On The Blockchain Network Before Requesting For The Specific Service. In This Framework The Consumer Of Service Sends A Request For A Service Or Resource To The Bdaas, Which Sends This Query To The Blockchain To Check Whether The Service Or Resource Requester Is A Legitimate User Or Not. And Finally, If Service Requester's Identity Is Authenticated By Blockchain Network Then Bdaas Provide The Service Which Is Requested To The Service Consumer.

Following Steps Demonstrate How The Service Requester Is Authenticated And Verified By

Bdaas Through Blockchain Network. It Is Also Demonstrated In Figure 5.

Process1: Steps For Taking Services From Bdaas

1. A Request Is Sent By The Service Requester To The Bdaas.
2. Bdaas Sends This Request To The Blockchain Network.
3. Blockchain Authenticates It.
4. Blockchain Network Response To The Bdaas In The Terms Of Ack Or Nak.
5. Bdaas Verify This Response.

6. Response Is Generated And Transmitted To The Servicerequester.
7. Service Requester Responses To The Bdaas.
8. Broadcast This Event And Transaction To The Blockchain Network And New Block Is Generated.

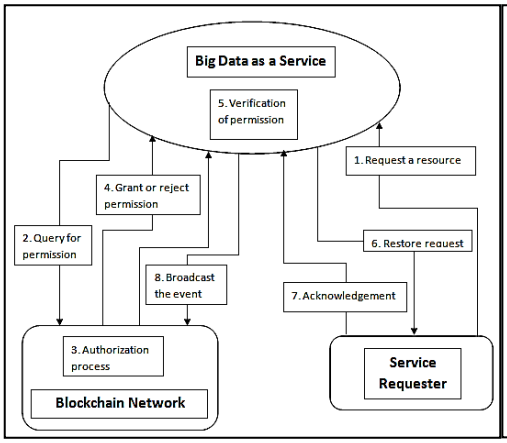

Fig5: Flow Diagram For Accessing Services From Bdaas

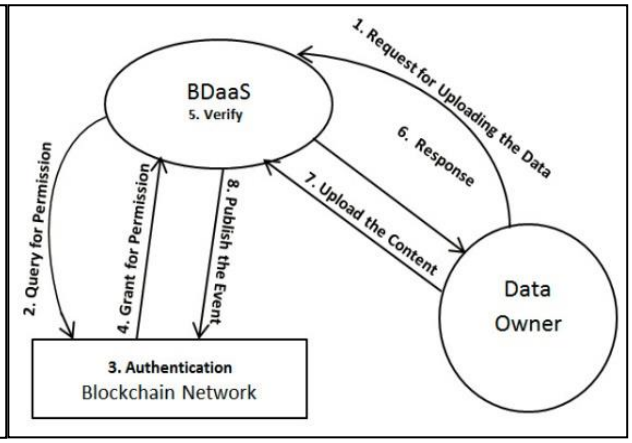

Fig6: Flow Diagram Of Uploading Data In Bdaas

At The Same Way In Process 2 Defines The Steps Involved In Granting The Permission To Upload The Data Contents By Data Owner To Bdaas Which Is Also Demonstrated In Figure 6.

Process 2: Steps For Uploading Data On Bdaas

1. Data Owner Sends The Request To The Bdaas For Uploading The Data Contents.
2. Bdaas Sends This Request To The Blockchain Network For Authentication.
3. Blockchain Authenticates This Request.
4. Blockchain Sends Response To The Bdaas.
5. Bdaas Verifies This Response.
6. Bdaas Sends Response To The Data Owner Or Producer.
7. Data Owner Now Uploads The Data Content After Getting Positive Response.
8. Broadcast This Event And Transaction In The Blockchain Network And New Block Is Created.

Analysis And Discussion

As We Know That The Current Internet Network Platform Architecture Is Based On The Centralized Server, Where All The Activities Of Internet Are Monitored By A Central Server. Therefore, The Security Of The User Contents Is Mostly Dependent Upon The Security Of Central Server. Different Kind Of Security Attacks Such As Dos, Ddos Attack, Sql Injection Attack, Etc Are Possible On The Central Server [41].

But Distributed Blockchain Network Allows That The Block Information Is Maintained By Each And Every Node In The Blockchain Network. In This Scenario Hackers Can Only Control Few Nodes Not All. And Also, The Information Stored In Blockchain Network Is Encrypted By Private Key Which Guarantees The Confidentiality Of The User's Data. If Any Kind Of Hacking Activity Is Reported Then The Consensus Model Of The Blockchain Network Will Ensure That That Activity Will Be Rejected.

Our Proposed Framework Will Work On The Principle Of Public Key Cryptography Where Log Information/Records Stored In Blockchainnetwork Are Secured Using Public Key Cryptography That Protects Against Any Kindof Possible Attacks For Modification Or Unauthorized Access. Also, Consumers And Data Producers Are Assigned With Their Private Key Through Which They Are Validated. To Ensure Data

Security And Track Access To The Stored Log Information, The Blockchain N/W Utilizes Digital Signature And Encryption Algorithms. Normally, Many Of The Consensus Algorithm Used In Blockchain Network Needs To Control At Least 51% Of The Network Nodes By An Attacker For Attempting Unauthorized Access And For Modifying The Records [42] Which Is Generally Impossible. Also, If An Attacker Wishes To Modifyany Block In Blockchain N/W, Each And Every Copy Of That Block In The Network Must Also Be Edited And All The Nodes Must Also Be Convinced That The Newly Created Block Is Valid, Which Is Impossible, Since Blocks Stored In The Blockchain Are Hashed.

Also, Our Proposed Framework Fulfills The Requirements Of Confidentiality, Integrity, Authenticity And Accountability.This Model Ensures That The User's Data Stored On The Bdaas Will Not Be Revealed To Or Used By Unlawful User. The Information Transmission Among Data Consumer, Data Owner, Blockchain And Bdaas Are Encrypted And Access Control Permission Among These Is Also Encrypted, Shows That The Nature Of Confidentiality. At The Time Of Data Uploading By The Authorized User, The User First Verified By The Blockchain Through Protection Mechanism. In This Way An Unauthorized User Or Bad System Administrator Can Not Enter Into The Network And Can Not Modify The User's Data. It Shows The Integrity Of The Data. Since All The Main Components Need To Be Verified And Trusted By Public Key And Private Key Combination In This Model, It Ensures The Authenticity Nature Of The Model. Here The Public Key Of The Data Owner, Consumer, Blockchain And Bdaas Is Publicly Available And At The Time Of Receiving The Information It Needs To Be Decrypted By The Private Key Of The Receiver. And At The Last This Model Keeps Track All The Log Information Of The Components In The Blockchain For The Security Analysis And Track Down The Entity Or Events Responsible For The Security Breaches.

Conclusion

In This Article We Have Proposed A Frameworkbig Data As A Service Platform To Enhance The Access Control And Privacy Using Blockchain Technology As A Tool. Since Protection Of User's Data And Data Modernization Is The Most Important Aspect In Any Organization. Also, Companies Need Timely And Targeted Analytics On Existing Big Data In A Secured Manner Which Can Easily Be Assured By Our Proposed System And Increase The Confidence Among The Companies Who Wish To Port To The Cloud. We Have Also Discussed The Security And Privacy Analysis On Our Proposed Framework. All The Transaction Log Data Is Stored On The Blockchain Network Which Ensures That Any Unauthorized User Or Even Service Provider Will Not Be Able To Perform Any Changes.So Many Companies Such As Google, Amazon, Microsoft, Oracle, Etc. Can Be Benefitted By Using Our Proposed Framework.This Framework Is Only A High-Level Design And Can Be Mathematically Validated In Future.Also,Machine Learning Algorithms Can Be Used As A Tool For Automatically Finding And Reporting The Suspicious Transaction.

References

[1] Z Zheng, J Zhu And Mrlyu. Service-Generated Big Data And Big Data-As-A-Service: An Overview. In *2013 Ieee International Congress On Big Data*, 2013; 403-410

[2] S Sahmimand H Gharsellaoui. Privacy And Security In Internet-Based Computing: Cloud Computing, Internet Of Things, Cloud Of Things: A Review. *Procedia Computer Science*, 2017; 112, 1516-1522.

[3] Mb Mollah, Mak Azad, Anda Vasilakos. Security And Privacy Challenges In Mobile Cloud Computing: Survey And Way Ahead. *Journal Of Network And Computer Applications*, 2017; *84*, 38-54.

[4] S Nakamoto. Bitcoin: A Peer-To-Peer Electronic Cash System. Available Athttps://Www.Bitcoin.Org/Bitcoin.Pdf.2008

[5] U Mukhopadhyay, Askjellum, O Hambolu, J Oakley, L Yu, And R Brooks. (2016, December). A Brief Survey Of Cryptocurrency Systems. In *2016 14th Annual Conference On Privacy, Security And Trust (Pst)* 2016; 745-752

[6] S Huh, S Cho, And S Kim. Managing Iot Devices Using Blockchain Platform. *In 2017 19th Internationalconference On Advanced Communication Technology (Icact)*2017; 464–467.

[7] A Dorri, Ss Kanhere, Rjurdak, And Pgauravaram. Blockchain For Iot Security And Privacy: The Case Study Of Asmart Home. In *2017 Ieee International Conference On Pervasive Computing And Communications Workshops(Percom Workshops)* 2017; 618-623.

[8] K Biswas, And V Muthukkumarasamy. Securing Smart Cities Using Blockchain Technology. In *2016 Ieee 18thinternational Conference On High Performance Computing And Communications; Ieee 14th International Conference On Smart City; Ieee 2nd International Conference On Data Science And Systems (Hpcc/Smartcity/Dss)* 2016; 1392-1393.

[9] M Turkanović, Mhölbl, K Košič, Mheričko, And Akamišalić. Eductx: A Blockchain-Based Higher Education Credit Platform. *Ieee Access*, 2018; *6*, 5112-5127.

[10] K Peterson, R Deeduvanu, P Kanjamala, Andk Boles.A Blockchain-Based Approach To Health Information Exchange Networks. In *Proc. Nist Workshop Blockchain Healthcare* 2016; 1, 1-10.

[11] E Xinhua, J Han, Y Wang, And L Liu. Big Data-As-A-Service: Definition And Architecture. In *2013 15th Ieee International Conference On Communication Technology* 2013; 738-742.

[12] Cloud Security Alliance (Csa). Security Guidance For Critical Areas Of Focus In Cloud Computing. Availableat:Https://Cloudsecurityalliance.Org/Guidance/Csaguide.V3.0.Pdf, Version 3, 2011.

[13] Cloud Security Alliance (Csa). The Notorious Nine: Cloud Computing Top Threats In 2013. Available At: Https://Cloudsecurityalliance.Org.

[14] C. Prybila*et Al.* Runtime Verification For Business Processes Utilizing The Bitcoin Blockchain. *Future Generation Computer Systems*, 2017.

[15] [15] Q Lu, And X Xu. Adaptable Blockchain-Based Systems: A Case Study For Product Traceability. *Ieee Software*, 2017; *34*(6), 21-27.

[16] Am Antonopoulos. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. " O'reilly Media, Inc." 2014.

[17] Z Zheng, S Xie, H Dai, X Chen, Andh Wang. An Overview Of Blockchain Technology: Architecture, Consensus, And Future Trends. In *2017 Ieee International Congress On Big Data (Bigdata Congress)* 2017; 557-564.

[18] Ic Lin, And Tc Liao. A Survey Of Blockchain Security Issues And Challenges. *Ij Network Security*, 2017; *19*(5), 653-659.

[19] Qh Vu,And R Asal. A Framework For Big Data As A Service. In *Digital Signal Processing (Dsp), 2015 Ieee International Conference On Digital Signal Processing* 2015; 492-496.

[20] S Khan, Ka Shakil, Sa Ali, And Malam. On Designing A Generic Framework For Big Data-As-A-Service. In *2018 1st International Conference On Advanced Research In Engineering Sciences (Ares)* 2018; 1-5.

[21] S Fugkeaw, Andh Sato. Privacy-Preserving Access Control Model For Big Data Cloud. In *2015 International Computer Science And Engineering Conference (Icsec)* 2015; 1-6.

[22] M Suriyapriya, And Ajoicy. Attribute Based Encryption With Privacy Preserving In Clouds. *International Journal On Recent And Innovation Trends In Computing And Communication*, 2014; *2*(2), 231-236.

[23] S Kumar, Sk Singh, Ak Singh, S Tiwari, And Rs Singh. Privacy Preserving Security Using Biometrics In Cloud Computing. *Multimedia Tools And Applications*, 2014; *77*(9), 11017-11039.

[24] S Namasudra. An Improved Attribute-Based Encryption Technique Towards The Data Security In Cloud Computing. *Concurrency And Computation: Practice And Experience*, 2019: *31*(3), E4364.

[25] S Namasudra, D Devi, Skadry, Rsundarasekar, And Ashanthini. Towards Dna Based Data Security In The Cloud Computing Environment. *Computer Communications*, 2020; *151*, 539-547.

[26] L Zhang, Y Cui, And Y Mu. Improving Security And Privacy Attribute Based Data Sharing In Cloud Computing. *Ieee Systems Journal*, 2019: *14*(1), 387-397.

[27] N Elisa, L Yang, F Chao, And Y Cao. A Framework Of Blockchain-Based Secure And Privacy-Preserving E-Government System. *Wireless Networks*, 2018; 1-11.

[28] A Chakravorty, And C Rong. Ushare: User Controlled Social Media Based On Blockchain. In *Proceedings Of The 11th International Conference On Ubiquitous Information Management And Communication*, 2017; 1-6.

[29] L Yue, H Junqin, Qshengzhi, And Wruijin. Big Data Model Of Security Sharing Based On Blockchain. In *2017 3rd International Conference On Big Data Computing And Communications (Bigcom)* 2017; 117-121.

[30] M Rehman, Za Khan, Mujaved, Mz Iftikhar, U Majeed, Ibux, And Njavaid, A Blockchain Based Distributed Vehicular Network Architecture For Smart Cities. In *Workshops Of The International Conference On Advanced Information Networking And Applications*, 2020; 320-331.

[31] Uu Uchibeke, Ka Schneider, Shkassani, Andr Deters. Blockchain Access Control Ecosystem For Big Data Security. In *2018 Ieee International Conference On Internet Of Things (Ithings) And Ieee Green Computing And Communications (Greencom) And Ieee Cyber, Physical And Social Computing (Cpscom) And Ieee Smart Data* 2018; 1373-1378.

[32] H Shekhawat, S Sharma, And Rkoli. Privacy-Preserving Techniques For Big Data Analysis In Cloud. In *2019 Second International Conference On Advanced Computational And Communication Paradigms(Icaccp)* 2019; 1-6.

[33] H Liang, J Wu, S Mumtaz, J Li, X Lin, And M Wen. Mbid: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection For V2x. *Ieee Communications Magazine*, 2019; *57*(10), 77-83.

[34] Y Zhang, R Deng, X Liu And D Zheng. Outsourcing Service Fair Payment Based On Blockchain And Its Applications In Cloud Computing. *Ieee Transactions On Services Computing*. 2018.

[35] J Li, J Wu, And L Chen. Block-Secure: Blockchain Based Scheme For Secure P2p Cloud Storage. *Information Sciences*, 2018; *465*, 219-231.

[36] E Gaetani, Laniello, R Baldoni, F Lombardi, Amargheri, And Vsassone. Blockchain-Based Database To Ensure Data Integrity In Cloud Computing Environments," In *Proc. Italian Conf. Cybersecuirity.*, Venice, Italy, Jan. 2017.

[37] Hg Do, And Wk Ng. Blockchain-Based System For Secure Data Storage With Private Keyword Search. In *2017 Ieee World Congress On Services (Services)* 2017; 90-93.

[38] Dk Tosh, S Shetty, X Liang, Ckamhoua, And Lnjilla.Consensus Protocols For Blockchain-Based Data Provenance: Challenges And Opportunities. In *2017 Ieee 8th Annual Ubiquitous Computing, Electronics And Mobile Communication Conference (Uemcon)* 2017; 469-474.

[39] L Yining, Zyuanjian, Lrushi, Tchunming. Blockchain-Based Verification Scheme For Deletion Operation In Cloud. *Journal Of Computer Research And Development*, 2018; *55*(10), 2199.

[40] Y Zhang, S Wu, Bjin, B And J Du. A Blockchain-Based Process Provenance For Cloud Forensics. In *2017 3rd Ieee International Conference On Computer And Communications (Iccc)* 2017; 2470-2473.

[41] C Simmons, C Ellis, S Shiva, D Dasgupta, And Q Wu. Avoidit: A Cyber Attack Taxonomy. In *9th Annual Symposium On Information Assurance (Asia'14)* 2014; 2-12.

[42] M Swan. *Blockchain: Blueprint For A New Economy*. "O'reilly Media, Inc.", 2015.