Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issues 3, pp. 407–424, DOI 10.12694:/scpe.v21i3.1737

ACCESS MANAGEMENT OF USER AND CYBER-PHYSICAL DEVICE IN DBAAS ACCORDING TO INDIAN IT LAWS USING BLOCKCHAIN

GAURAV DEEP *, JAGPREET SIDHU †, AND RAJNI MOHANA ‡

Abstract. Computing on the cloud has changed the working of mankind in every manner, from storing to fetching every information on the cloud. To protect data on the cloud various access procedures and policies are used such as authentication and authorization. Authentication means the intended user is access data on the cloud and authorization means the user is accessing only that data for which he is allowed. The intended user now also includes Cyber-Physical Devices. Cyber-Physical Devices share data between them, fetch data from cloud. Cloud data is managed by employees of cloud Companies. Persons sitting on the cloud managing companies data is always doubtful as so many insider attacks have happened in the past affecting the company Image in the market. Data Related to Cyber-Physical Space may come under Insider attack. Companies managing user data are also liable to protect user data from any type of attack under various sections of the Indian IT act. Work in this paper has proposed blockchain as a possible solution to track the activities of employees managing cloud. Employee authentication and authorization are managed through the blockchain server. User authentication related data is stored in blockchain. Authorization rules are written in any Role/Attribute-based access language. These authorization rules stores the data related to user requests allowed access to data in blockchain. Proposed work will help cloud companies to have better control over their employee's activities, thus help in preventing insider attack on User and Cyber-Physical Devices.

Key words: Cryptography, Transmission Control Protocol, Single sign-on, Internet of Thing, Policy enforcement Point, Timestamp, Nonce, Policy Decision Point, Internal Threat Detection Unit.

AMS subject classifications. 94A60

1. Introduction.

Cloud Computing Revolutionized Data storage to Processing in every area of science and technology. International Data Corporation (IDC)[21] released a study on the Global Data sphere, which says it will grow to 175 Zettabytes by 2025. Data is shared and accessed every moment throughout the world. In data storage and sharing Cloud plays an important role. Every cloud model through the world Follows Standards laid down by the National Institute of Standards and Technology (NIST). Cloud data is stored as well as shared on-demand with the help of configurable computing resources [41]. Digital Data on the Cloud is stored, which may represent any type of form of Information such as Images, Sound, Video, Database, etc.

Cloud Database means Database stored over the cloud, which offers various services to the users such as storing, modifying and making it available anywhere in the world. To maintain the Privacy of data, It Is Important to Protect Cloud Databases [53]. According to the CIA Principle, security concerns mainly deal with Confidentiality, Integrity, and Availability. Security Concerns covers Attacks from within and from outside the Organization, Issues related to Consistency Management, Access Control, Network Breaches, Resource Exhaustion, etc. are also covered [7].

Insider threat means threats originating from Employees of the organizations, These Employees have been provided Access rights to access the internal system, thus violating the Internal System organization security policy. Outsider threats try to release the confidential information out in the real world, which defaces the organization. When the Care Taker of Various Services of Cloud Computing tries to Steal Users Data it becomes more difficult to prevent it [38]. Cloud Database is no different from such a scenario where its numerous advantages supersede its disadvantages/Loopholes, these Loopholes cannot be ignored when it has affected in the past so much to the working of many Organizations whether it maybe Yahoo, Facebook, and Google.

*Research Scholar, Department of CSE & IT, JUIT, Solan, India
†Assistant Professor(Senior Grade), Department of CSE & IT, JUIT,Solan, India
‡Associate Professor,Department of CSE & IT, JUIT, Solan, India (rajni.mohana@juit.ac.in).

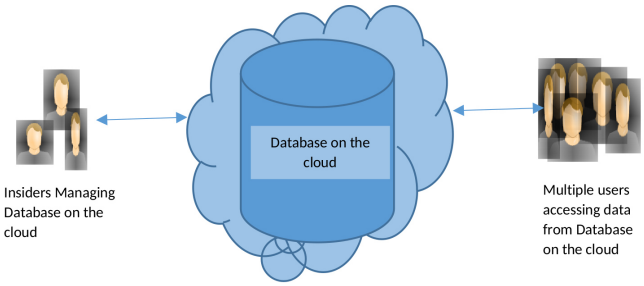

FIG. 1.1. *Role of Insider and users on the Database on the cloud*

Intensions of these Staff members to monitor User and its data activity is always doubtful due to many insider attacks happened in the past. A Survey in this regard From U.S. State of Cybercrime in the year of 2016 [8] represented, Electronic crimes suspected to be caused by insiders is of 27%. According to this survey, 33 Percent of the Respondents Agreed that Insider attack is more Dangerous than Outsider Attack.

The number of Insiders depends on the amount of data they are manging over the cloud as shown in Figure 1.1. Insiders are also Employees of the Organization. They can take advantage of the information of how and where data is protected to do insider attacks.

Existing User Authentication Techniques Suffers from Various Attacks and Threats. User Password Can be guessed and Two Factor Authentication Using Short Message Service (SMS) also suffers from Attacks, as Code sent on SMS can be tracked by the Attacker on the network [49].Authentication codes from Google were sent by Google Authenticator to respective users via SMS as these Codes are difficult to Cracked but Security Breach to Google could lose all User Authentication Codes.

Organization of this paper. The rest of the paper is as follows, Authentication techniques available for outsiders and insiders to the cloud are covered in Section 2. It also covers various authorization policies available for users. Section 3 covers various sections available under the Indian IT Act. This section also covers details of sections dealing with various aspects of the Cloud. Section 4 covers Detail and working of Blockchain. This section also covers details of application areas of Blockchain. Section 5 covers Need of Transaction Authentication Mechanism for Access Management in Database as a Service (DBaaS) according to Indian IT Laws. Section 6 Covers Transaction Authentication Mechanism using Blockchain to store Every Transaction Detail according to Indian IT Laws. Experiment Results of Proposed Work were shown in Section 7. Finally in Section 8 Paper is concluded.

2. Authentication and Authorization of User.

Importance of Access Control Can be understood from the fact that many researchers tried to explore this field so that only legitimate users can access his data. User access control consists of two main components, Authentication and Authorization as shown in Figure 2.1.

This section discusses primarily Authentication and Authorization of Insiders and Outsiders on the cloud.

2.1. Authentication of the user.

2.1.1. Authentication techniques of the outsider users. The purpose of Authentication is to allow access only to the intended user. Work from Many researchers on Outsider threat is compared and shown in

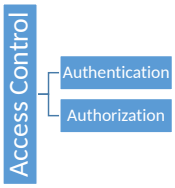

FIG. 2.1. *Access Control Components*

TABLE 2.1
Contrasting Authentication Techniques for Outsider User

	Authentication Type	Single sign-on	Technique used	Suitable for Resource constraint IOT	Mutual Authentication	Multi-Owner Authentication
Tsai et al.[49]	Three factor	Yes	Elliptic curve cryptography	No	Yes	No
Kalra et al.[31]	Two Factor	No	Elliptic curve cryptography	Yes	Yes	No
Amin et al. [3]	Multi-Factor	No	Bio Hashing	No	Yes	No
Yang et al. [55]	Two Factor	Yes	Delffie-Hellman	No	No	No
Kumari et al. [33]	Multi-Factor	No	Elliptic curve cryptography	Yes	Yes	No
Shajina and Varalakshmi [45]	Two Factor	Yes	Triple DES	No	Yes	Yes
Anakath et al.[4]	Multi-Factor	No	Simple-Homomorphic Encryption	No	No	No
Chaudhary et al. [15]	Three factor	Yes	Elliptic curve cryptography	No	Yes	No
Kumar et al.[32]	Biometric	No	Elliptic curve cryptography	No	Yes	No
Chatterjee et al.[13]	Biometric	No	Clustering	No	Yes	No

Table 2.1. Authentication Process for a user means that allows only legitimate users to access their data and restricts various hackers to attacks.

Tsai et al. [49] had proposed Authentication Scheme for mobile users. This scheme allows to use single private key for accessing cloud services from multiple service providers. Public and Private keys for the user as well as for the service provider are generated by Smart card generator so that they can authenticate each other . Smart card allows users to access services from the service providers. This scheme benefits in providing user anonymity, user un-traceability, mutual authentication, and key exchange.

Kalra et al.[31] had proposed mutual authentication protocol For Internet of Thing (IoT) devices and cloud servers This scheme uses Hypertext Transfer Protocol (HTTP) cookies to implement Secure Elliptic curve cryptography (ECC). Internet of thing Devices uses Cloud Services to enhance their Processing Capabilities. To get Authenticate with the server, embedded devices should work as HTTP Client. Transmission Control Protocol/Internet Protocol (TCP/IP) Protocol Stack is used to configure embedded devices. Three phases are available in this Protocol from Registering Devices in First Phase,Getting Log-in them in second Phase and Authenticate them in the last Phase. This Scheme Provides Resistance to various types of attacks such as brute force attack, eavesdropping, man-in-the-middle attack, offline dictionary attack, cookie theft attack, replay attack and provides forward secrecy, anonymity, confidentiality, and mutual authentication.

Amin et al. [3] had proposed User Authentication for a multi medical server system using User-id, Password, Biometric template like fingerprint and smart card. First, the user chooses his desired identity, Password and Biometric template like fingerprint and sends them through a Secure channel for user Registration. After receiving User details and Applying Bio Hashing on them, data is stored in the User Smart card as well as in User Registration Medical Server. Once the user is authenticated he is allowed to fetch data from the desired Medical Server according to his requirement. This scheme Prevents Session key discloser attack, User Impersonation Attack, replay attack, enables early wrong password detection and provides Mutual authentication, Resists off-line password guessing attack.

Yang et al.[55] had proposed a Protocol for allowing access to multimedia data on the multimedia cloud. This Protocol uses Two-factor authentication with Open ID which requires smart cards along with user Login

details. Various Cloud models were used in this scheme for achieving Authentication of Smart cards and Users. User Authorization policies were based on Role-Based Access Control (RBAC). To validate this work various analysis was done like on security, Functionality, and Efficiency.

Kumari et al. [33] had proposed Authentication scheme for IoT and Cloud Servers. This scheme is uses Multi-Factor like login details, Cookies and device details along with Temper resistant device, Elliptic curve cryptography which helps in preventing various types of attacks like the absence of device anonymity, Insider attack, Offline Password guessing, and No session key computation. This Authentication Protocol is suitable for Resource constraint IOTs where mutual authentication is required.

Shajina and varalakshmi [45] had proposed protocol for Multi Owner Authentication, this protocol works on multiple owners, Group manager and service manager in a cloud for authentication and increases the Security requirement of Single sign-on. The Proposed mechanism allows the main owner to create a group and is allowed to add other members along with their access permissions. Owners are provided with a valid token after certified by a Certification authority with all required parameters .A Valid token Consist of all the details of User credentials, Token expiration time, services granted, etc., session tokens from session manager will allow these services to access.

Anakath et al. [4] proposed Trust Model for authentication, in this device identity is identified and authentication Protocol is selected. For authentication purposes, Knowledge, Possession and Inherence factors can be used. This protocol uses Possession factors, One Time Passwords, and passwords that users know only. A user profile is created on Big Data Multi-Factor Cloud Authentication (MACA) with user details and user Parameters in encrypted form.

Chaudhary et al. [15] had proposed an Improved User Authentication Scheme. This scheme uses a single private key for authenticating mobile users, allowing them to use services from multiple cloud service providers. This work is an improvement work of Tsai[49]. This paper prevents the Server Forgery attack at the time of the Authentication phase. Proposed work is much more secure, robust and is validated in ProVerif.

Kumar et al. [32] had proposed authenticating cloud users using Face features i.e by Bio-metrics based recognition. Encryption is used on Bio-metric Database which stores Facial features of cloud users. Facial Features of users are extracted from pre-processed face images. These Facial Features helps in recognition of users. Scores of Facial features are calculated and it is matched with the stored similarity scores of facial features on the cloud.

Chatterjee et al. [13] proposed a re-authentication system based on Bio-metrics, This system is better and enhances security level by using keystroke dynamics over Password based authentication mechanism. In this Scheme User is asked to enter Log-in details for authentication Purposes. When User enter's his credential for authentication , his Keystroke Dynamics are stored in Database. These details will help in identification and verification,which are extracted by a k-means clustering algorithm. Tests were conducted on Heterogeneous, Homogeneous, and Aggregate feature sets.

2.1.2. Authentication techniques of insider user. To safeguard user data on the cloud and accessed by only legitimate user various user authentication techniques have been discussed, there is a need to protect user data from insiders on the cloud also. Behavioral analysis is the area where many researchers have worked for designing authorization policies for insiders. Table 2.2 shows a comparison of many approaches that have worked on Insider Threat.

In the paper of Wu et al. [53] have proposed making the understanding of User Data difficult for insiders by applying Encryption. Data is Decrypted first before applying query on the user data, in the end encryption is done again. Feature index extraction is applied to user data before encryption proposed by authors. It also helps in making a query on the cloud. Encryption was done with Index Generator, Query translator helps in making Feature Index of user data and Query Executor executes the query.

Moon et al. [38] introduced two-tier architecture for analyzing the behavior of Insider . They have also proposed In-Memory Database (IMDB) for a database protection system. Work done by Insiders are saved in Log Files known as Change Audit Log. Database log Pre-processor pre-processes the log File.This File is further sent to Insider Behavior Analysis Server. This insider behavior analysis Server analysis and detects any availability of Attack. Cloud Capability is also incorporated in this.

Yaseen and Panda [57, 58, 56] have contributed three papers on the detection and prevention of Insider

Table 2.2
Contrasting Authentication Techniques against Insider Attack

	Insider Action Monitoring	Authorization rules Modification based on Insider Action Monitoring	User-Machine probity	Authenti-cation of Insider	Availability of encryption on User Data before querying on Cloud
Wu et al. [53]	No	No	No	No	Yes
Moon et al. [38]	Yes	Yes	No	No	No
Yaseen et al. [57][58][56]	Yes	Yes	No	No	No
Dou et al. [23]	Yes	Yes	Yes	No	No
Shaghaghi et al.[44]	Yes	Yes	No	No	No
Chatto-padhyay et al. [14]	Yes	No	No	No	No
Baracaldo et al. [6]	Yes	Yes	No	No	No
Meng et al. [36]	Yes	No	No	No	No
Babu et al.[5]	Yes	Yes	No	Yes	No
Eberz et al. [24]	Yes	No	No	Yes	No

attack. In their First work [57] Insider threat prediction and its prevention measures have been proposed, Insider knowledge is analyzed by using a knowledgebase Algorithm that also considers Constraint Dependency, Hot Cluster, Safe Cluster, and Dependency Matrix. By using this Algorithm Knowledge Graph is generated which helps in protecting Insider Attack. Threat Prediction Graph was proposed in the second work [58] by using the knowledgebase Algorithm. In third work, authors have proposed Architecture with Multiple Policy Enforcement Points (PEP's) and Single Policy Decision Point (PDP) to detect insider threats.In this architecture alogrithims proposed in previous works were used. This system is suitable to work when the number of PEPs is less in number.

Dou et al. [23] have proposed an authentication protocol for Hadoop with a Trusted platform. This protocol helps in removing the limitations of user authentications and insider attacks in Kerberos. Authentication keys and its operations were locally hidden in this Protocol. This Protocol is bounded with specific Systems. It stores current software and hardware details of the hosting machine in an internal set of platform configurations registers. This Proposed protocol helps in securing specific systems against insider attacks.

Shaghaghi et al. [44] have proposed Gargoyle Software Defined Network (SDN) architecture. The proposed work was designed to detect and deter suspicious activities of insider using SDN. It also analyzes Passive Network traffic and retrieves contextual information. Mainly three components were proposed in this architecture Network Context Analyser, Risk Management, and Advanced Enforcement Point. Various Risks were detected and actions can be planned accordingly based on insider activity details. This detail is extracted by monitoring network traffic.

Chattopadhyay et al. [14] have proposed Time-series classification of insider activities. In this work Insider behavior analysis was done on tracking single day activities. This analysis was done from a single day to over some time for detecting insider threats. Statistics were collected to detect malicious or non-malicious insider based on behavioral analysis. Classification technique two-layered deep autoencoder neural network is applied to improve the results.

Baracaldo et al. [6] proposed the Geo-Social Insider Threat Resilient Access Control Framework (G-SIR). In this proposed work Insider movement activities are monitored. This monitoring helps in classifying insiders into enablers, inhibitors or neutral. Risky users come in the category of Inhibitors. Trusted users come in the category of enablers and average users based on Risk level comes in the category of neutral. This framework uses PEP-PDP Model along with Monitoring, Context, Inference and Access control Module. Role-based access control (RBAC) is used to write Permissions and Roles.

Meng et al. [36] have proposed a technique to prevent Medical Smartphone Network from an Insider attack, where it can leak Patient information malicious devices are detected based on behavioral profiling. Nodes in the

TABLE 2.3
Comparison of Different Authorization Policies framework used in Distributed Environment.

	Authorization Policy framework used	Environment used	Application
Abomhara et al. [1]	WBAC (Team-based)	Distributed	Healthcare
Alam et al. [2]	GRBAC	Distributed	Cloud
Habiba et al. [27]	iCanCloud simulation platform	Distributed	Cloud
Sun-Moon Jo [30]	XML	Distributed	Mobile
Chen et al. [16]	RBAC	Distributed	Healthcare
Shin et al. [46]	Bilinear pairings, Strong Diffie–Hellman representation, Linear encryption	Distributed	Cloud
Gabillon et al. [26]	ABAC	Distributed	Pub-Sub Network For IoT
Rathore et al. [42]	Answer Set Programming	Distributed	Online Social Network

MSN are connected to the Central server, each node in the network sends its Statistics based on the user working on the Medical smartphone. Working Profile of each node is created on the central server. A malicious node on the network is detected by the difference in Euclidean distance between two behavioral profiles. Evaluations were carried out in Real-world MSN with the help of a Practical healthcare center.

Babu et al. [5] have proposed a technique to prevent Insider attack on the cloud by Analysing the Behaviour of the Insider and associating Risk-based access control. Behavior analyses are done by using Keystroke Dynamics. Risk analyses are done in an offline manner with the associated resource. Every object is assigned a value of risk. These Risk Values are stored in a database called resource repository. For Behavioral analyses, Support vector machine is used. If a Malicious user is detected in the system it's all Privileges are revoked.

Eberz et al. [24] have proposed a technique to prevent Insider Threat in an Organization by detecting Eye Movement biometrics. In this work, researchers have identified a set of 20 features of an eye by which user authentication can be done in a transparent continuous manner. Video-based gaze tracking is used to track eye movement. Experiments were conducted in a controlled manner in a Lab on 30 Persons from the general public. Persons were asked to perform various activities on the screen to study eye movement and various other parameters. Open set and closed set classifiers are applied to the retrieved data set. Experiments were repeated after some time to test the time stability of the proposed features.

2.2. Authorization of users. To allow a user to access data is decided under Authorization policy. Along with Authentication, Authorization policy plays a very important role. Various Authorization Policies framework used in Distributed Environment is discussed in Table 2.3 along with their application area.

Abomhara et al. [1] have proposed a work-based access control (WBAC) model with a team role classification based on the Belbin team role theory. Teams in WBAC models are segregated based on Thought, action, and management based on their contributions to collaborative work. Proposed work has been suggested for cooperative healthcare environments. In a Particular scenario Multiple Doctors from multiple Departments and hospitals working as a team on a patient.

Sharing and Access to the healthcare record of a patient with Multidisciplinary team consultants need Authorisation control, as leakage of sensitive data may happen by insiders. Authors have first formalized the model with basic elements and relations, defined various authorization constraints and access control decision functions for WBAC Model. This work reduced the complexity level of Permission reviews as compared to Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

Alam et al. [2] have proposed Garbled role-based access control (GRBAC) in the cloud. The concept of Garbled Circuits (GC) and Fully Homomorphic Encryption (FHE) are used in Garbled computation. This Garbled computation is used in Role-based access control (RBAC) making it into GRBAC. Permissions to user access are associated with their respective assigned roles. All the details of user roles are stored in the RBAC server. An attacker is not able to know the roles even if the GRBAC is compromised. It helps in Providing Strict Security in Cloud Environment.

Habiba et al. [27] have proposed the Dynamic Access control system in the cloud. This Dynamic Access control system consists of mainly four models namely the Data access right model, Policy model, Access control

management model and Authorization model. The data access right model consists of access rights tree, in which Access rights are represented by access rights and the hierarchical relationship between two access rights is represented by edges.

Policy model classifies Policies into different categories obligations (O), conditions (C), primary rules (R), deadline (D) and user preferences (F). Policies must represent there Subject (S), a requested access right (A), a resource (Rs), a set of rules (R) and a preference (F). Every policy must be expressed with 8 –Tuple (S, A, Rs, R, C, O, D, F). Access control management model consists of Many Sub Models handling many key areas like Request Management, Communication, User Management, Data Management Module, Monitor, etc. Authorization model consists of three stages where decision making is performed as Pre, On-Going, and Post-stage of data access along with credit level checking of the user.

Sun-Moon Jo [30] have proposed a secure access policy method for Dynamic Extensible Markup Language (XML) data environment. The author is working on Resource Efficient Secure Access Policy in which access to data is allowed according to Privilege Information, Security Policy, Authorization Policy, and Propagation Policy. In this paper it focuses only on the accessible area as element units in the target document, on these element units very small access policies are applied. This Policy accesses parts of the target document allowing every small access policy to work on the whole target document.

Chen et al. [16] have proposed community medical Internet of things (CMIoT) for medical data. Privacy protection of medical data in healthcare is provided in terms of transmission protection, storage protection, and access control. Transmission protection is provided by asymmetric encryption, storage protection is provided by symmetric encryption and access control is provided by identity authentication and Dynamic authorization based on the role under which access is applied. In community medical Internet of things (CMIoT) data from various IoTs are collected at the gateways further Multi-Path fragmented, encrypted and sent to Cloud for storage. This cloud data is allowed to access by the user according to his predefined Role. Dynamic Authorization allows data to be fetched only from Third Party Cloud of community medical Internet of things.

Shin et al. [46] have proposed the Anonymous Authentication and Authorization (AAnA) scheme. There proposed work uses short traceable signatures. In this scheme, two authorities are simultaneously working one is a group manager and another is the authorization manager. This scheme achieves anonymity by having two different managers for Group membership and Authorization. The role of the Group Manager is to provide Group membership based on Short traceable signatures. Authorization manager provides Privileges to users based on their real identity, Authorization list of all users along with their Privileges is forwarded to Service provider. At any time the Service provider detects Illegal activity it will ask the signature from the user, which is passed to the Group manager and Authorization manager for further necessary action.

Gabillon et al. [26] have proposed a highly expressive attribute-based access control (ABAC) security model. This Model is used for the Message Queuing Telemetry Transport (MQTT) protocol. MQTT Protocol is used for Publisher-subscriber Network for the Internet of Things. Whenever publisher Publishes Messages in various topics, subscribers get messages under the topics for which they are subscribed. This Paper assumes only one Trusted Broker is working in MQTT Protocol. This paper also assumes to be working on TLS/SSL at the Transport layer between all nodes of the IoT network. Authors have used first-order logic with equality to define the proposed model. The access control enforcement system in the proposed model uses Policy Enforcement Point (PEP), a Policy Decision Point, a Policy Information Point (PIP—contextual database), and a Policy Administration Point (PAP). Logical Security policies for this model are defined in the Resource Description Framework (RDF).PEP intercepts all the MQTT requests and forwards them to PDP, PDP Takes help from PIP in deciding the access and saves the results in PIP.

Rathore et al. [42] have proposed an access control model for online social networks. This control model works on resources shared by Single or Multiple Parties on Online Social network. Privacy suffers on Social Network as Resources is shared by multiple times, some times without the consent of Owners. In this model Trust level is calculated Among Each Owner of the Resource. Access Policy among owners Depends upon trust level, as trust is higher among Family members and lower in Normal friends. The proposed model is logically represented by using Answer Set Programming.

3. Indian IT Laws for Privacy Threat. To prevent data threat on the cloud, many protocols were designed and implemented it can be seen From Tables 2.1-2.3. To prevent data from theft IT Laws plays a

TABLE 3.1
Indian IT Acts on Electronic Data and its Management

Sections based on concerned issues	Section According to Indian IT Act 2000	Amended Section According to Indian IT Act 2008	Rule According to Indian IT Act 2011
Retention of electronic records.	7	7 7A	
Secure electronic record	14	14	
Certifying Authority to follow certain procedures	30	30C 30CB	
Penalty for damage to the computer, computer system, etc.	43	43 43A	
Tampering with computer source documents.	65	65	
Hacking with the computer system.	66	66 66C 66F	
Protected system	70	70A 70B	
Confidentiality and Privacy breach	72	72A	
Responsibility of service provider and authorized agents			7
Account Audit and Information System details of the service provider and authorized agents			8

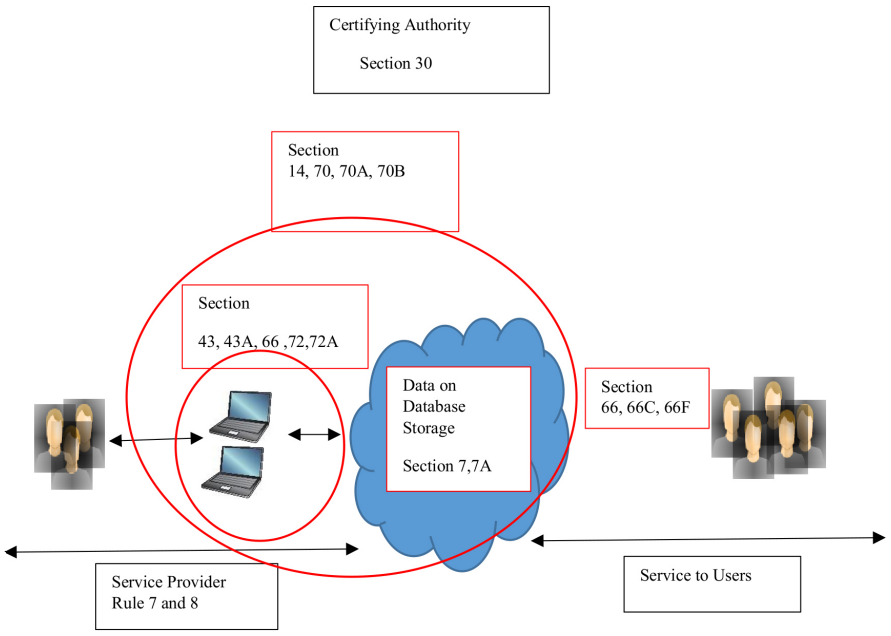

FIG. 3.1. *Role of various IT Act sections Data and IT Resources*

major role, but their role is limited when Laws differ from country to country. Indian government brought Indian IT ACT 2000 [9] in this regard in the year 2000, later amendments were done in 2008 [10] on Electronic Data and its Management is shown in Table 3.1.

Various points are provided related to the Retention of Electronic Records, Secure Electronic Records, and Certifying Authority Followed Procedure, etc. They are shown in Figure 3.1 and explained below in detail:

Section 7, Retention of electronic records in its original generated format is only allowed when it is required to keep electronic records for a certain period for subsequent reference with all document origin, desti-

nation date and time of dispatch or receipt details. This point was amended in IT act 2008 as Section 7A Audit of Documents etc. in Electronic form there is a provision for audit of documents, records or processed information /unprocessed information.

Section 14, Secure electronic record by this it means that any security procedure applied on the electronic record to keep it secure during at a specific point of time then that Electronic record is said to be Secure electronic record from such point of time to the time of verification.

Section 30, Certifying Authority to follow procedures from making use of IT Infrastructure to get secure from intrusion and misuse, Providing Reliability in various services and functions, To Follow all security procedures to ensure that the secrecy and privacy of the digital signatures are assured and to observe such other standards as may be specified by regulations. Some new points are added in this in IT Act 2008, a repository of all Electronic Signature Certificates issued under this Act are to be maintained and publish information regarding its practices, Electronic Signature Certificates and current status of such certificates.

Section 43, Penalty for damage to the computer, computer system, by any unauthorized person tries to access, retrieve any form information, corrupts the system with a virus, any sort of damage to the system he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. Manipulation or theft to data in any form is also considered as damage to the data in IT ACT 2008.

The new subsection to this is also added as "43 A Compensation for failure to protect data". When a corporate body is unable to manage sensitive data which it owns making wrongful gains to someone then that Corporate is liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Section 65. Tampering, destroying, concealing or any form of damage to computer source documents, source code is done knowingly or intentionally, when it is required to be maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Section 66. Hacking with the computer system, Any Person who hacks the system Manipulates or deletes any information residing in a computer resource shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. New sub Sections to this is also added in IT Act 2008 as:

Section 66C Punishment for identity theft. Under this point who so ever does any type of Identity theft, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66F Punishment for cyber terrorism. Under this point who so ever with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by unauthorised access and any sort of damage to any computer resource or Computer database or Cybercrime using such conduct causes Losses to Human Beings or Property or adversely affect the critical information infrastructure in specified under section 70 shall be punishable with imprisonment which may extend to imprisonment for life.

Section 70, Protected system. The government may notify any Computer system/Computer Network as a Protected system accessed by authorized personnel only. Unauthorized access to the protected system shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

In IT Act 2008 this point Protected system is referred to as Critical Information Infrastructure means the computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety. The government should follow various security procedures to secure Critical Information Infrastructure. New subsections to this is also added in IT Act 2008 as:

Section 70 A, National nodal agency. The government may designate any organization as National Nodal agency which shall be responsible for all measures including Research and Development relating to the protection of Critical Information Infrastructure.

Section 70 B, Indian Computer Emergency Response Team to serve as a national agency for incident response.

The government may designate any government agency as the Indian Computer Emergency Response Team with all the required staff. This team will work on various elements of Cyber incidents and Cybersecurity. Any service provider, intermediaries, data centers, body corporate or person who fails to provide the information called for shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.

Section 72, Penalty for breach of confidentiality and privacy. Any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and discloses them to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. In IT Act 2008 Definition of Any Person also consists Intermediary in Section 72 A. Imprisonment for a term which may be extended to three years, or with a fine which may extend to five lakh rupees, or with both.

In 2011 New IT rules were issued [11]:

Rule 7. Responsibility of service provider and authorized agents: The government may direct every service provider and authorized agent to keep every detail of electronic services delivered and the said records shall be produced for inspection and audit.

Rule 8. Account Audit and Information System details of the service provider and authorized agents:- Government may direct every service provider and authorized agents to go for Audit on regular intervals .To check various parameters of security, confidentiality and the privacy of information. The performance of any software application used in the electronic service delivery is also checked .The accuracy of accounts kept by the service providers and authorized agents is maintained . These service providers and authorized agents must rectify the defects and deficiencies pointed out by the audit agencies within the time limit specified by the audit agency.

Due to the declaration for protecting the data of every individual transaction and citizen is to be submitted by every service providers and the authorized agents. Protected data should not be disclosed to any one in unauthorized way without the written consent of either the individual or the appropriate Government. Otherwise, the Government is allowed to take necessary action under section 45, and can debar such service providers and the authorized agents.

4. Blockchain. Blockchain provides numerous benefits in terms of Security. Every technological area wants to take advantage of it. Blockchain provides the benefit of Immutability, Forgery Resistant, Democratic, Double-Spend Resistant, Consistent State of the Ledger, Resilient and Auditable [39, 34]. Immutability means once a transaction is done on the Blockchain it cannot be altered. Every Node in the Blockchain Cryptographic hash and digital signatures are used to make it Forgery Resistant. Every node in the Blockchain should have equal rights like in Democratic structure, no one is powerful than others. Preventing double spend in Blockchain is done by allowing to access every transaction up to the genesis block. All nodes in the Blockchain are Auditable, all previous nodes are accessible via a hash function.

Blockchains are of three types: Public, Private and Consortium Blockchain. In Public Blockchain anybody can Participate, whereas in Private Blockchain authorized user is allowed to participate in a controlled manner by a centralized authority. As in Private Blockchain Number of users are in Finite Numbers it is less complex as compared to Public Blockchain. In the Consortium Blockchain, the consensus process is controlled by a pre-selected set of nodes, these selected nodes control the authorization of nodes.

Each node in Blockchain is connected to its previous node, backward to the first node (Genesis Node) in the distributed network. Each node stores the Hash value of the previous node, by which it is checked membership of Blockchain. Various parameters are stored in each node of Blockchain like Index value, the Hash value of the previous node, Timestamp value, Merkle tree root hash, Data, Nonce value is shown in Figure 4.1.

It is getting difficult to change Blockchain Previous Node parameters as it grows. Blockchain has helped in numerous applications in achieving the Desired Security level. Table 4.1 shows various solutions proposed by Blockchain in various key areas.

Chen et al. [17] have proposed the use of Blockchain in the education sector. All academic details of a student are to be stored in the Blockchain including assignments, exam results and Degree details to prevent Fraud in education, which can be accessed by student ID. Blockchain can be used as learning as Earning, Digital

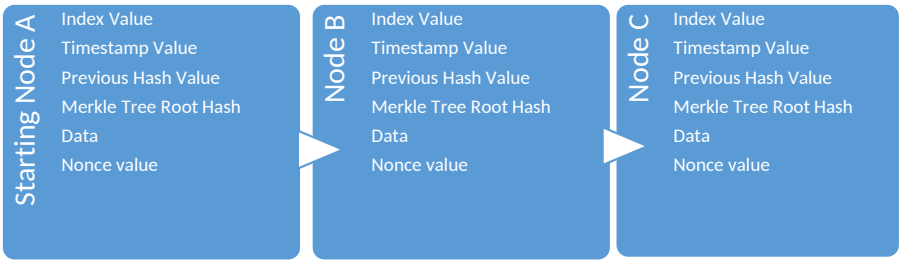

FIG. 4.1. *Blockchain Nodes with Stored Parameters*

TABLE 4.1
Research Issues with the use of Blockchain as the solution

	Deal with issues	Solution proposed
Chen et al. [17]	Fraud in Education	Student Education detail in Blockchain
Li et al. [35]	Bottleneck issue and chances of compromising centralized management server in VANET	Decentralized VANET with all data in Blockchain
Chung et al. [18]	Customized Product Process Management is difficult to maintain in Cognitive Manufacturing	Blockchain is used to maintain Data of Process Management in Cognitive Manufacturing
Sun et al. [48]	Trust issues in sharing based Smart cities	Blockchain can be used for trust-building in sharing based smart cities
B.Vinod [52]	Issue of interline charges, Bonus on genuine bookings to agents by airline and tracking of booking for a property becomes a tedious task when multiple sites are used for bookings	Blockchain can help in maintaining a single record for interline charges, the record of bookings and record of bookings for a property.
Han et al. [29]	Patient Health Data storage in a centralized system is prone to cyber-attacks.	Patient Health Data storage is done in Hybrid Blockchain, in Private Blockchain at the local Hospital and Consortium Blockchain at the Upper level. Hybrid Blockchain makes things difficult for an attacker.
Ryu et al. [43]	Digital forensics involves a very lengthy and difficult procedure in IoT for sent messages	IoT digital forensics is made simpler with the use of Blockchain

Currency can be rewarded for Smart contracts between students and teachers. The same can be applied to Teachers and schools where Teachers are rewarded with Digital currency based on their performance based on teaching activities.

Li et al. [35] have proposed the use of Blockchain in the area of Vehicle Adhoc network (VANET). Traditionally VANET works in a centralized system where it is controlled by the single management authority. The centralized system becomes a threat to its members once it is compromised by an attacker. Also, the Centralized system is prone to a single point of failure due to excessive load and bottleneck problems. To prevent centralized systems from the excessive load and bottleneck problem authors proposed to use a decentralized system with Blockchain. Vehicles are moving on the road in groups, their Parameters like speed, location, etc. are communicated to the Roadside unit by onboard unit installed in the vehicle. The roadside unit transfers these real-time vehicle parameters to the Certification Authority and other servers in the core network. All Data available in the core network is stored in Private Blockchain to make it more secure.

Chung et al. [18] have proposed the use of Blockchain in the area of Cognitive Manufacturing. Day by day competition in the market is increasing, Companies have started to attract customers by offering personalized customization on products. These customizations on products increase raw materials variety, so many changes in process management. All data generated from product customization to manufacturing to delivery is stored in a blockchain.it helps in understanding customer trends and demand. Sensors used in the manufacturing

process are used for monitoring purposes. Data generated by these sensors are stored in Blockchain and can be accessed to detect any deviation in the required parameters.

Sun et al. [48] have proposed Blockchain in Sharing based smart cities. Blockchain can be used in basically Human, organization and technology in building trust in smart cities. To build trust in Sharing Transactions made by humans, Blockchain plays an important role. Data received from various IOT's in smart cities can be stored with the help of Blockchain builds trust in sharing based Services among businesses. Security provided by Blockchain builds trust in decentralized nodes, either may be used for transactions, IOT's or Services is sharing based smart cities.

B. Vinod [52] has proposed the use of Blockchain in Business related to Travelling. Loyalty bonuses for an airline can use digital tokens which can be accessed by using cryptocurrency. Interline charges are converted to cryptocurrency which can be taken by the next airline. Private Blockchain can be used for contracts between airlines and agents for tracking records of sales which helps in secure payments. The issue is raised when a property is booked by multiple sites. To eliminate this problem Blockchain can be used which helps in tracking the booking record of a property. Smart contracts can be generated using machine learning and stored in Blockchain.

Han et al. [29] have proposed the use of Blockchain storing medical records of patients in a hospital. In the Hospital chain, every Hospital stores Patient Health data in their centralized server, which is a soft target for cyber-attacks like WannaCry ransomware attack. To prevent Cyber-attacks patient data can be stored in de-centralized form using Hybrid Blockchain. Patient Health Data is stored in Private Blockchain at the Hospital level, if the patient allows it to share among other entities of the Hospital chain it is further stored in Consortium Blockchain. Two Blockchains are working one at the Hospital level and the other is at the Hospital chain level providing more security in the de-centralized Form.

Ryu et al. [43] have proposed to use Blockchain for IOT Digital Forensics. With the technological advancement with time, Exponential Growth of IoT's had happened. IoT can Communicate with each other as per requirement, in Cloud, on Network or directly. For Digital Forensics All three areas Cloud, Network and devices can be explored. Diversification of IoT's Type and usage has made Digital Forensics difficult. Authors have proposed Blockchain to store communication details of IOT's by which Digital Forensics is possible in a refined manner. Blockchain can be accessed by any one of the Participants Device user, Device Manufacturer, Service Provider and Investigator for Digital Forensics.

5. The need for User and Cyber-Physical Device Transaction Authentication Mechanism . User accesses its stored data from Cloud Databases, Performance of cloud database depends upon the architecture it is following. Policies to be implemented on Cloud Databases is decided by PDP, and are enforced by PEP. The best suitable architecture for Cloud databases is De-centralized (Distributed Network) based as shown in Figure 5.1.

Cloud Data storage to Manipulation related services is provided by Cloud service providers to various sections of users. According to the Indian IT act all the issues of Data and Resource management is to be managed by Service Provider. If any issue related to data privacy to data leakage comes then it is the responsibility of the Service provider to take care of. For better control of data, every organization tries to achieve better control in authentication and authorization by using various policies as shown in Table 5.1.

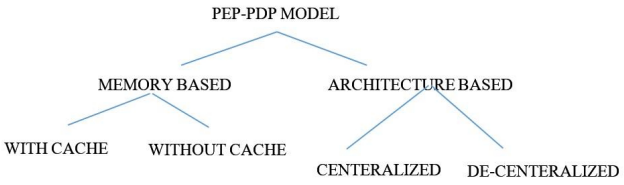

FIG. 5.1. *PEP-PDP Model types*

TABLE 5.1
Various Authentication and Authorization Policies Available

Under Indian IT Laws	
Various Authentication Policies available are	Various Authorization Policies available are
Elliptic curve cryptography	WBAC (Team-based)
Bio Hashing	GRBAC
Delffie-Hellman	iCanCloud simulation platform
Triple DES	XML
Simple-Homomorphic Encryption	RBAC
Clustering	ABAC

As the data Sharing between Cyber-Physical space [37, 28] is increasing day by day, there is a need to check the Privacy of data. The requirement to Modify existing Access and Authorization Policies is the need of time. Under the Indian IT act 2008 and its various amendments, it is the responsibility to keep track and maintain all transaction logs for any future need for this Section 7 and section 14 is provided, which says to keep track of all electronic transactions securely.

Whenever a request is received at DbaaS Cloud it should be able to differentiate between Request is from User or Cyber-Physical Device. Existing Rules Stored in PEPs are not applicable when requested data is from Cyber-Physical devices. Access Control Policies [12, 50] should be able to handle requests from Cyber-Physical Device. Every request to data is to be scanned and a new Rule is required to allow access to data. Whenever many Cyber-Physical Devices are requesting access to data, Existing systems are not able to handle requests at a large scale as proposed in [56]. There is a requirement to store every transaction done at DbaaS Cloud and the system should be able to handle a Large Number of Requests.

6. Proposed User and Cyber-Physical Device Transaction Authentication Mechanism (U & CPD TAM). Every authentication and authorization policy achieves its intended purpose up to a certain level when we see statistics of Data leakage and user Privacy crimes [25, 40, 47]. For better management of user data on Distributed networks in Cloud Databases, Management of user data is to be controlled by the technique which is based on Distributed networks. Blockchain can help in providing better control in terms of user authentication and authorization as shown in Table 6.1 as required in Section 7 and 14 Under Indian IT Act 2008 and its amendments.

Requests to access Data from User and Cyber-Physical Device is received at DbaaS Cloud, Insiders at the DbaaS cloud can Access to data illegally and can take benefits. The benefits of blockchain in this regard can be viewed in [51, 60, 59]. Blockchain server can keep an eye on Insider activities from Log-in to User Authorization. Insider Log-in Control Protocol using Blockchain is already published in our previous paper [22].Blockchain server also stores the data of user authorization as well as logs in detail. In any case, Insider tries to change Authorization Rules, its activity is stored in the Blockchain node as User Transaction data as shown in Figure 6.1.

Blockchain will help in monitoring the activities of Insider From authentication to authorization. Any uneven activity can be easily tracked and responsibility can be fixed with evidence. Each Request to access data from Insider goes to PEP which allows Access to data only if the rule for data access is available for that Insider. If Rule is not available at PEP, that request to access data from an insider is forwarded to PDPs, To

TABLE 6.1
Use of Blockchain at different levels

<table>
<tr><td colspan="4">Request to Access Data from User / Cyber-Physical Device</td></tr>
<tr><td colspan="2">Authentication</td><td colspan="2">Authorization</td></tr>
<tr><td>Insider</td><td>Outsider</td><td>Insider</td><td>Outsider</td></tr>
<tr><td colspan="2">Blockchain Technique For User Authentication</td><td colspan="2">Authorization Technique with Blockchain for Authorization Policy Request Tracking</td></tr>
<tr><td colspan="4">Blockchain server for cloud database for Section 7 and 14
(Indian IT Act 2008 and its amendments)</td></tr>
<tr><td colspan="4">Under Indian IT Laws</td></tr>
</table>

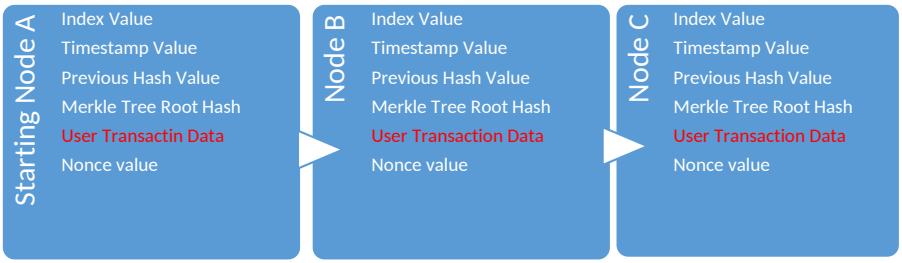

FIG. 6.1. *User Transaction Data in Blockchain Node*

Track each request for particular data, Blockchain can be used along with PDPs.

In our Proposed Algorithm 1, Working of the Dependency checkpoint and Internal threat Detection unit proposed in [57, 58, 56] in their research work is same we have introduced the concept of Distributed PEP-PDP Model along with Blockchain Servers for tracking every request forwarding between PEPs and PDPs For better control according to Section 7 and 14 Under Indian IT Act 2008 and its amendments.

Algorithm 1 Insider Threat Prevention Algorithm for Distributed PEP-PDP Environment with side caching Model

Input: An Insider Alice request Q for accessing a data item D, Q (Alice D), the PEP that receives Alice request, request may be forwarded to other other PEPs in the System S=PEP1, PEP2,.....PEPn, along with these common caches (CPEP1, CPEP2,...., CPEPn), Dependency checkpoint DCP available at designated PDP for each set of PEPs.

Output:Access Decision (Grant or Reject)

1: If Q (Alice, D) does not exist in corresponding PEP Cache then Go to Step 2 else Go to Step 5
2: If Q (Alice, D) does not exist in other PEP Cache then Go to Step 3 else Go to Step 4
3: Forward Alice request to Designated PDP by Calling Algorithm 2
4: Fetch Q (Alice, D) and Forward it to Corresponding CPEP Cache and Go to Step 5
5: Send Request D to Dependency-CheckPoint for checking Dependencies and Go to Step 6
6: If D can be combined with K to infer information then Go to Step 7 else Go to Step 9
7: If Check Alice has a cached value of K then it may be a possible threat then Forward Alice request to Designated PDP by calling Algorithm 2 else Go to Step 8
8: If Alice is not the cached value of K No threat found, re-issue the PEP cache response for Alice request to D then Go to Step 9
9: If D cannot be combined with K to infer information No threat found, then re-issue the PEP cache response for Alice request to D

Algorithm 2 PEP Request Authentication using Blockchain Mechanism.

Input:Request Q received at Blockchain Server of Designated PDP Server for each PEP, It checks for Q Request is from PEP.

Output:Access Granted or Rejected to‘ PEP Request by Bloackchain Server

1: If Request == PEP then Go to Step 2 else Go to step 5
2: If Login ID & Signature == Valid then continue this step else Go to step 5
3: If current index value > Last stored index vale & Hash value & Timestamp value & Nonce value== Valid then Create New Blockchain node with requested transaction details and Go to Step 4 else Go to step 5.
4: Grant Authentication with Update to a user record in Blockchain Database and Send Request to PDP Server by Calling Algorithm 3
5: Give error message and Exit

Algorithm 3 PEP Request is forwarded to Designated PDP Server.

Input:Request Q received at Designated PDP Server for each PEP, It Checks for Possible threat at ITDU

Output:Request Approved or Rejected

1: If Designated PDP, using the ITDU, decides that there are no threat exists then Alice is allowed to get his/her requested D, all CPEPs receive Designated PDP decision and Corresponding CPEP allows the user to get his requested D. else Go to Step 2

2: If Designated PDP, Using ITDU decides that a threat exists then Alice is not allowed to get his/her requested D,Request is rejected by Designated PDP.Response is updated in all CPEPs

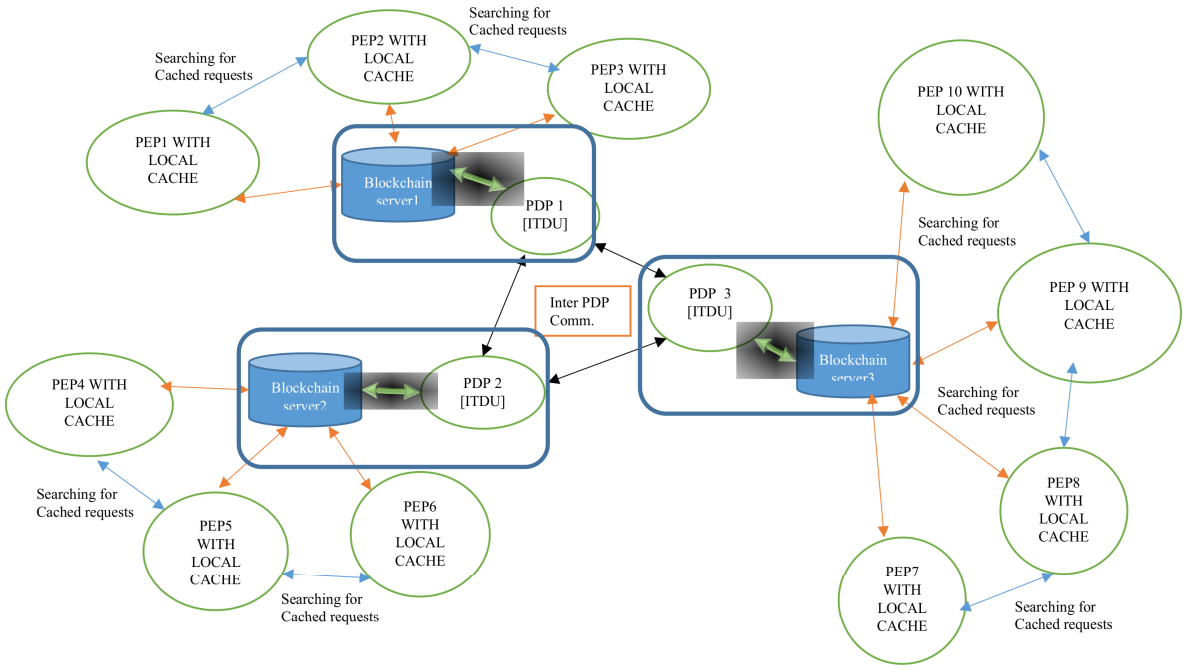

FIG. 6.2. *Working of Proposed Private Blockchain Servers PEP-PDP Architecture*

Blockchain will also help in tracking every request coming from PEPs to its designated PDP. The detailed proposed architecture is shown in Figure 6.2. For every Request from Insider to PEP, it is checked at the Dependency checkpoint for possible threat, if no threat was detected then Insider is allowed to access data according to cached Copy at PEP otherwise request to access data is forwarded to Designated PDP. First at PDP Side request is received by Blockchain Server where it was checked for authenticity by checking PEPs UID and Signature. If it was valid then a new node is created at Blockchain to track all details of the transaction and request is forwarded to Designated PDP. If it was Found Invalid, Request from PEP is rejected and an error message is conveyed.

The benefit of using Multiple PDPs is to have Better Scalability and better Response Time as compared to Existing architecture proposed in [56]. Better control of transactions can be achieved by using Blockchain Server where detail about any transaction can be fetched.

7. Experimentation Results. The proposed architecture is checked on the Verification and Validation Formal Tool Scyther by using Asymmetric keys. Each PEP to PDP communication is done by using Asymmetric keys. This Formal Tool verifies the proposed Protocol against all the Security Protocols. Whenever this tool detects any Attack in the proposed Protocol it creates an attack graph for better understanding. For having the best Security Requirements in place it uses Four Claims namely Alive, Nisynch, Secret and Commitment

BlockchainPEP_PDP	PDP1	BlockchainPEP_PDP,a1	Secret kira	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a11	Secret kirb	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a13	Secret kirc	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a	Nisynch	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a2	Alive	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a3	Commit PDP1,t	Ok	No attacks within bounds.
	PDP2	BlockchainPEP_PDP,PDP21	Secret kird	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP22	Secret kire	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP23	Secret kirf	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP24	Nisynch	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP25	Alive	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP26	Commit PDP2,t	Ok	No attacks within bounds.
	PDP3	BlockchainPEP_PDP,PDP31	Secret kirg	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP32	Secret kirh	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP33	Secret kirii	Ok	No attacks within bounds.
		BlockchainPEP_PDP,a14	Secret kirj	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP34	Nisynch	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP35	Alive	Ok	No attacks within bounds.
		BlockchainPEP_PDP,PDP36	Commit PDP3,t	Ok	No attacks within bounds.
	PEP1	BlockchainPEP_PDP,i1	Secret kiri	Ok	No attacks within bounds.
		BlockchainPEP_PDP,i	Nisynch	Ok	No attacks within bounds.
		BlockchainPEP_PDP,i2	Alive	Ok	No attacks within bounds.
		BlockchainPEP_PDP,i3	Commit PDP1,t	Ok	No attacks within bounds.
	PEP2	BlockchainPEP_PDP,ii1	Secret kirb	Ok	No attacks within bounds.
		BlockchainPEP_PDP,ii	Nisynch	Ok	No attacks within bounds.

FIG. 7.1. *The Output For the Scyther Claim Test for Multiple PDPs and PEPs*

[19, 20, 54]. Intended Communication is achieved by having some events that are described as "Alive". Nisynch stands for non-injective synchronization, it means that the receiver receives the messages from the sender in a synchronized manner. Commitment is a promise that is made by one party to the other. The confidentiality of data is achieved by using Claim Secret.

Results of the Proposed Protocol in Scyther are shown in Figure 7.1. It can be seen from the Result that Status is Ok which means there are No Attacks within Bounds. All four claims Alive, Nisynch, Secret and Commitment are achieved and verified. In this Proposed, Protocol 10 PEPs along with 3 PDPs and 3 Blockchain servers are tested against possible attacks.

8. Conclusion. Effective control of data on the cloud is the need of the hour. Many companies ran into losses due to data theft on the cloud. According to the Indian IT act Company managing Cloud is responsible for data theft occurred on the cloud. Employees working in companies may steal data from the cloud and put the company in a bad image. To control the activities of Employees in cloud managing companies, a strong mechanism is required. This Paper proposes Blockchain as a solution to control the activities of Employees from authentication to Authorisation. Request for Data Access from User and Cyber-Physical Device is Received at DbaasS Cloud. Policies to data Access are managed by Cloud Employees. Employees can take advantage, for performing Insider Attack.

To have better Control under section 7 and 14 under the Indian IT Act and its amendments this paper proposes the concept of Distributed PEP-PDP Model along with Blockchain Servers for tracking every request forwarding between PEPs and PDPs. Each Transaction between PEP and PDP is now tracked with the possible results. The proposed Protocol is tested on Scyther Formal Tool for possible attacks. From the results, it is concluded that the proposed system is highly efficient and robust. The proposed system is ready to be implemented in the actual scenario by providing better control of transactions between PEPs and PDPs. In future work, work will focus on better transaction control on the PEP side itself using Blockchain.

REFERENCES

[1] M. Abomhara, H. Yang, G. M. Køien, and M. B. Lazreg, *Work-based access control model for cooperative healthcare environments: Formal specification and verification*, Journal of Healthcare Informatics Research, 1 (2017), pp. 19–51.

[2] M. Alam, N. Emmanuel, T. Khan, Y. Xiang, and H. Hassan, *Garbled role-based access control in the cloud*, Journal of Ambient Intelligence and Humanized Computing, 9 (2018), pp. 1153–1166.

[3] R. Amin and G. Biswas, *A novel user authentication and key agreement protocol for accessing multi-medical server usable in tmis*, Journal of medical systems, 39 (2015), p. 33.

[4] A. Anakath, S. Rajakumar, and S. Ambika, *Privacy preserving multi factor authentication using trust management*, Cluster Computing, 22 (2019), pp. 10817–10823.

[5] B. M. Babu and M. S. Bhanu, *Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud*, Procedia Computer Science, 54 (2015), pp. 157–166.

[6] N. Baracaldo, B. Palanisamy, and J. Joshi, *G-sir: an insider attack resilient geo-social access control framework*, IEEE Transactions on Dependable and Secure Computing, 16 (2017), pp. 84–98.

[7] T. Bhatia and A. Verma, *Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues*, The Journal of Supercomputing, 73 (2017), pp. 2558–2631.

[8] H. Bleau, *Current state of cybercrime in 2016*. rsa.com, 2016.

[9] P. by Government of India, *The information technology act, 2000*. meity.gov.in, 2000.

[10] ———, *The information technology(amendment) act, 2008*. meity.gov.in, 2009.

[11] ———, *The information technology rules,2011*. meity.gov.in, 2011.

[12] Y. Cao, Z. Huang, Y. Yu, C. Ke, and Z. Wang, *A topology and risk-aware access control framework for cyber-physical space*, Frontiers of Computer Science, 14 (2020), pp. 1–16.

[13] K. Chatterjee et al., *Biometric re-authentication: An approach towards achieving transparency in user authentication*, Multimedia Tools and Applications, 78 (2019), pp. 6679–6700.

[14] P. Chattopadhyay, L. Wang, and Y.-P. Tan, *Scenario-based insider threat detection from cyber activities*, IEEE Transactions on Computational Social Systems, 5 (2018), pp. 660–675.

[15] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash, and T. Shon, *An improved anonymous authentication scheme for distributed mobile cloud computing services*, Cluster Computing, 22 (2019), pp. 1595–1609.

[16] F. Chen, Y. Luo, J. Zhang, J. Zhu, Z. Zhang, C. Zhao, and T. Wang, *An infrastructure framework for privacy protection of community medical internet of things*, World Wide Web, 21 (2018), pp. 33–57.

[17] G. Chen, B. Xu, M. Lu, and N.-S. Chen, *Exploring blockchain technology and its potential applications for education*, Smart Learning Environments, 5 (2018), p. 1.

[18] K. Chung, H. Yoo, D. Choe, and H. Jung, *Blockchain network based topic mining process for cognitive manufacturing*, Wireless Personal Communications, 105 (2019), pp. 583–597.

[19] C. J. Cremers, *The scyther tool: Verification, falsification, and analysis of security protocols*, in International conference on computer aided verification, Springer, 2008, pp. 414–418.

[20] C. J. F. Cremers, *Scyther: Semantics and verification of security protocols*, Eindhoven University of Technology Eindhoven, Netherlands, 2006.

[21] J. R. David Reinsel, John Gantz, *The digitization of the world from edge to core*. seagate.com, 2018.

[22] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, *Authentication protocol for cloud databases using blockchain mechanism*, Sensors, 19 (2019), p. 4444.

[23] Z. Dou, I. Khalil, A. Khreishah, and A. Al-Fuqaha, *Robust insider attacks countermeasure for hadoop: Design and implementation*, IEEE Systems Journal, 12 (2017), pp. 1874–1885.

[24] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, *Looks like eve: Exposing insider threats using eye movement biometrics*, ACM Transactions on Privacy and Security (TOPS), 19 (2016), pp. 1–31.

[25] J. Foster, *1 terrifying cyber crime statistics*. dataconnectors.com, 2018.

[26] A. Gabillon, R. Gallier, and E. Bruno, *Access controls for iot networks*, SN Computer Science, 1 (2020), p. 24.

[27] M. Habiba, M. R. Islam, A. S. Ali, and M. Z. Islam, *A new approach to access control in cloud*, Arabian Journal for Science and Engineering, 41 (2016), pp. 1015–1030.

[28] V. Hahanov, *Cyber physical computing for IoT-driven services*, Springer, 2018.

[29] H. Han, M. Huang, Y. Zhang, and U. A. Bhatti, *An architecture of secure health information storage system based on blockchain technology*, in International Conference on Cloud Computing and Security, Springer, 2018, pp. 578–588.

[30] S.-M. Jo, *Secure access policy for efficient resource in mobile computing environment*, Journal of Computer Virology and Hacking Techniques, 13 (2017), pp. 297–303.

[31] S. Kalra and S. K. Sood, *Secure authentication scheme for iot and cloud servers*, Pervasive and Mobile Computing, 24 (2015), pp. 210–223.
[32] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh, *Privacy preserving security using biometrics in cloud computing*, Multimedia Tools and Applications, 77 (2018), pp. 11017–11039.
[33] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, *A secure authentication scheme based on elliptic curve cryptography for iot and cloud servers*, The Journal of Supercomputing, 74 (2018), pp. 6428–6453.
[34] K. H. Kwak, J. T. Kong, S. I. Cho, H. T. Phuong, and G. Y. Gim, *A study on the design of efficient private blockchain*, in International Conference on Computational Science/Intelligence & Applied Informatics, Springer, 2018, pp. 93–121.
[35] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, *Blockchain meets vanet: An architecture for identity and location privacy protection in vanet*, Peer-to-Peer Networking and Applications, 12 (2019), pp. 1178–1193.
[36] W. Meng, W. Li, Y. Wang, and M. H. Au, *Detecting insider attacks in medical cyber–physical networks based on behavioral profiling*, Future Generation Computer Systems, (2018).
[37] D. P. Möller, *Introduction to cyber-physical systems*, in Guide to Computing Fundamentals in Cyber-Physical Systems, Springer, 2016, pp. 81–139.
[38] C. S. Moon, S. Chung, and B. Endicott-Popovsky, *A cloud and in-memory based two-tier architecture of a database protection system from insider attacks*, in International Workshop on Information Security Applications, Springer, 2013, pp. 260–271.
[39] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, *Blockchain. business & information systems engineering, 59 (3), 183–187*, DOI: http://dx. doi. org/10.1007/s12599-017-0467-3, (2017).
[40] M. Powell, *11 eye opening cyber security statistics for 2019*. cpomagazine.com, 2019.
[41] U. D. o. C. Published by NIST, *Nist cloud computing standards roadmap*. nist.gov, 2018.
[42] N. C. Rathore and S. Tripathy, *A trust-based collaborative access control model with policy aggregation for online social networks*, Social Network Analysis and Mining, 7 (2017), p. 7.
[43] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, *A blockchain-based decentralized efficient investigation framework for iot digital forensics*, The Journal of Supercomputing, 75 (2019), pp. 4372–4387.
[44] A. Shaghaghi, S. S. Kanhere, M. A. Kaafar, E. Bertino, and S. Jha, *Gargoyle: A network-based insider attack resilient framework for organizations*, in 2018 IEEE 43rd Conference on Local Computer Networks (LCN), IEEE, 2018, pp. 553–561.
[45] A. Shajina and P. Varalakshmi, *A novel dual authentication protocol (dap) for multi-owners in cloud computing*, Cluster Computing, 20 (2017), pp. 507–523.
[46] S. Shin and T. Kwon, *Aana: Anonymous authentication and authorization based on short traceable signatures*, International journal of information security, 13 (2014), pp. 477–495.
[47] R. SOBERS, *110 must-know cybersecurity statistics for 2020*. varonis.com, 2020.
[48] J. Sun, J. Yan, and K. Z. Zhang, *Blockchain-based sharing services: What blockchain technology can contribute to smart cities*, Financial Innovation, 2 (2016), pp. 1–9.
[49] J.-L. Tsai and N.-W. Lo, *A privacy-aware authentication scheme for distributed mobile cloud computing services*, IEEE systems journal, 9 (2015), pp. 805–815.
[50] M. Uriarte, J. Astorga, E. Jacob, M. Huarte, and O. López, *Survey on access control models feasible in cyber-physical systems*, in Cyber-Physical Systems: Architecture, Security and Application, Springer, 2019, pp. 103–152.
[51] B. van Lier, *Blockchain technology: The autonomy and self-organisation of cyber-physical systems*, in Business Transformation through Blockchain, Springer, 2019, pp. 145–167.
[52] B. Vinod, *Blockchain in travel*, Journal of Revenue and Pricing Management, 19 (2020), pp. 2–6.
[53] Z. Wu, G. Xu, C. Lu, E. Chen, F. Jiang, and G. Li, *An effective approach for the protection of privacy text data in the clouddb*, World Wide Web, 21 (2018), pp. 915–938.
[54] H. Yang, V. A. Oleshchuk, and A. Prinz, *Verifying group authentication protocols by scyther.*, JoWUA, 7 (2016), pp. 3–19.
[55] T.-C. Yang, N.-W. Lo, H.-T. Liaw, and W. C. Wu, *A secure smart card authentication and authorization framework using in multimedia cloud*, Multimedia Tools and Applications, 76 (2017), pp. 11715–11737.
[56] Q. Yaseen, Y. Jararweh, B. Panda, and Q. Althebyan, *An insider threat aware access control for cloud relational databases*, Cluster Computing, 20 (2017), pp. 2669–2685.
[57] Q. Yaseen and B. Panda, *Predicting and preventing insider threat in relational database systems*, in IFIP International Workshop on Information Security Theory and Practices, Springer, 2010, pp. 368–383.
[58] ———, *Insider threat mitigation: preventing unauthorized knowledge acquisition*, International Journal of Information Security, 11 (2012), pp. 269–280.
[59] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, *Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems*, IEEE Access, 6 (2018), pp. 12295–12303.
[60] D. Zhaoyang, L. Fengji, and G. Liang, *Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems*, Journal of Modern Power Systems and Clean Energy, 6 (2018), pp. 958–967.

Edited by: Anand Nayyar
Received: Apr 13, 2020
Accepted: May 21, 2020