ENHANCING DATA SECURITY THROUGH BLOCKCHAIN

S. LALITHADITHYA [1]
Student, CSE (AI)
Dr. M.G.R Educational And Research Institute
Chennai, India
Solletilalithadithya3@gmail.com

SYED MOHAMMED YASEEN [2]
Student, CSE (AI)
Dr. M.G.R Educational And Research Institute
Chennai, India
syedmohammadyaseen2@gmail.com

S. MANJITH YADAV [3]
Student, CSE (AI)
Dr. M.G.R Educational And Research Institute
Chennai, India
Manjithyadav75@gmail.com

Dr. P.S. RAJAKUMAR[4]
Professor, Dept. of CSE
Dr. M.G.R Educational And Research Institute
Chennai, India

DR.T.V. ANANTHAN[5]
Professor &HOD(AI), Dept. of CSE
Dr. M.G.R Educational And Research Institute
Chennai, India

DR.K.S. RAMANUJAM[6]
Professor, Dept. of CSE
Dr. M.G.R Educational And Research Institute
Chennai, India

Abstract — Blockchain technology brings significant advantages like transparency, immutability, and decentralization, making it a reliable solution for secure data storage, verification, and access control. This research delves into essential components such as cryptographic encryption, smart contracts, and consensus protocols, ensuring a secure, tamper-resistant, and verifiable system for handling sensitive information. Additionally, it explores real-world applications in industries like healthcare, finance, and supply chain management, demonstrating how blockchain enhances data confidentiality, integrity, and accessibility.However, this intensive approach is associated with considerable risk.centralized servers are susceptible to cyber attacks where hackers can steal, modify or delete important legal data, leading to irreversible losses.we propose the management of legal and criminal documents related to blockchain technology. With integrated security features, distributed memory and review mechanisms, blockchain prevents data integrity, increases unauthorized changes, and improves overall security. This shift provides a more transparent, manipulated and more resilient system to protect sensitive legal records

Keywords— Blockchain technology, Decentralized storage, Data security, Transparency, Immutability, Smart contracts, Cryptographic encryption, Consensus protocols, Tamperproof.

I. INTRODUCTION

In today's digital age, legal document management represents a critical challenge, especially due to weaknesses associated with centralized servers. These servers, often managed by administrators, are susceptible to operations and cyberattacks, leading to data integrity and security breaches. Unrecognized changes directly exacerbate concerns about the reliability and reliability of legal documents. To address these urgent issues, our project suggests a paradigm shift for the use of blockchain technology in the management of legal and criminal documents. In distributed storage, each data record is replicated through several nodes, ensuring resistance to individual point errors. In the case of a node error, the service is accessible through other functional nodes, which increases reliability and continuity. Additionally, blockchain ensures data security through internal encryption mechanisms, protecting sensitive information from unauthorized access and operations. When storing a new data record, the blockchain checks the integrity of the previous block by recalculating the hash code. Manipulation of data leads to unavailable contracts and allows you to recognize unauthorized changes. With the help of Solidity programming, intelligent

contracts are designed to promote seamless inte raction with blockchain networks. These intellig ent contracts include the capabilities to store an d access legal documents to ensure efficient and secure treatment of confidential information.

II. LITERATURE REVIEW

The literature on A prototypical smart contract (wrapped as a decentralized application) is presented to investigate the potential benefits of applying Blockchain to Logistics, Application for Logistics is used for blockchain real-world application. [1]. secure, decentralized, trusted cyber infrastructure solution for future energy systems, Then, a Blockchain-based smart grid cyber-physical infrastructure model is proposed [2].

Usage-based Insurance (UBI) for vehicles determines the insurance premiums according to actual usage and driving pattern A Private and Decentralized Usage-Based Insurance Using Blockchain [3]. Decentralized learning involves training machine learning models over remote mobile devices, edge servers, or cloud servers while keeping data localized SPDL: Blockchainsecured and Privacy-preserving Decentralized Learning [4]. The smart grid idea was implemented as a modern interpretation of the traditional power grid to find out the most efficient way to combine renewable energy and storage Blockchain Technology on Smart Grid, Energy Trading, and Big Data: Security Issues, Challenges, and Recommendations. [5].

User, content, and device names as a security primitive have been an attractive approach, especially in the context of Information-Centric Networking (ICN) architectures. Decentralized Name-based Security for Content Distribution using Blockchains [6]. Presents architectural design, interactions, logic flow, algorithms, and implementation details, along with cost, computation, and security evaluation. Decentralized Access Control for IoT Data, hashing for encryption as well as decryption and Trusted Oracles [7].

The rapid development of cloud storage has greatly promoted industrial productivity and social progress. However, with the era of big data coming, there exist 2021 10 several challenges for cloud storage in terms of the difficulty of maintaining data security. several challenges for cloud Efficient Identitybased Proxy Reencryption Scheme in Blockchainassisted Decentralized Storage System. [8] The border gateway protocol (BGP) has become the myriad of infrastructure of the Interne t as a typical interdomain routing protocol. DRRS BC: A decentralized routing registration system ba sed on blockchain. [9].You cannot efficiently store large files on the blockchain. On the one hand, bl ockchains are bulging with data that needs to be di stributed within blockchain networks. Blockchain-based decentralized access control for IPFS.[10]. It illustrates the potential for blockchain transform ation beyond cryptocurrency, highlighting the use of funding, supply chains and land registrations. T he impact of electricity, import and infrastructure on the overall emissions emissions check blockch ain application using case studies and expert analy sis. [11]. Blockchain offers many benefits, includi ng decentralization, sustainability, anonymity, and monitorability. CO2 footprints in general sector, blockchain challenges and opportunities. [12] Blockchain technology is a connected, systematic chain of blocks containing transaction history and other user data. [13]. Purely peer-to-peer version o f electronic cash allows you to send online payme nts directly from one party to another without goi ng through a financial institution

This literature review identifies various approache s researchers have developed to improve AI image generation, model robustness, and ethical conside rations. The current project is based on this progre ss by implementing clip embedding for semantic o rientation, image loyalty,and various data magnifi cation techniques, to develop a more integrated an d more accurate diffusion model. This combinatio n of strategies aims to improve known distortions within the generated AI. This contributes to the re sponsible delivery of generation technology in rea l-world applications.

III. EXISTING SYSTEM

In the current system, legal and criminal documen ts are managed using centralized servers controlle d by administrators. This centralized approach ma kes data susceptible to manipulation and unauthor ized access. Administrators have the authority to modify documents and declare concerns about the reliability and integrity of records. Furthermore, c entralized servers are susceptible to cyber attacks, leading to data injuries and loss. Recognizing cha nges to a document is a challenge because there is no direct mechanism for checking. Overall, existi

ng systems lack robust security measures and resis tance to malicious activities, representing substant ial risks to the confidentiality and reliability of leg al documents.

A . Challenges in Existing Systems

While existing systems offer valuable capabilities, they often share common challenges:

- Centralized Management Simplifies administration and access control.
- Familiar Infrastructure: Utilizes established server technology for documents storage.
- Ease of maintenance: Centralized server can be maintained and updated more efficiently.
- Cost-Effective: Initial setup costs may be lower compared to blockchain implemention.
- Integration: Existing systems may be integrated with other software solutions more seamlessly.

IV. Network Protocol

Introduction

The Decentralized Secure Data Transmission Protocol (DSDTP) is a network protocol that ensures secure, tamper-proof, and decentralized data transmission using blockchain technology. Unlike traditional client-server architectures, DSDTP eliminates single points of failure and provides a trustless, verifiable, and transparent framework for data security.

Network Architecture

The network consists of several entities working together:

1. Blockchain Nodes

Nodes maintain a distributed ledger storing data access records and integrity proofs. Use consensus mechanisms such as Proof of Stake (PoS) or Proof of Authority (PoA) to validate transactions.

2. Data Providers (Storage Nodes)

Provide secure encrypted data storage. Utilize IPFS (InterPlanetary File System) or decentralized storage networks (e.g., Filecoin, Arweave).

3. Data Requesters (Client Nodes)

Request access to data securely. Authenticate using decentralized identity mechanisms (DIDs, Zero-Knowledge Proofs).

4. Smart Contracts

Enforce access control policies for data retrieval. Automate authentication, authorization, and logging.

Protocol 1 Generating a compound identity

1: **procedure** COMPOUNDIDENTITY(u, s)
2: u *and* s *form a secure channel*
3: u executes:
4: $(pk^{u,s}_{sig}, sk^{u,s}_{sig}) \leftarrow \mathcal{G}_{sig}()$
5: $sk^{u,s}_{enc} \leftarrow \mathcal{G}_{enc}()$
6: u *shares* $sk^{u,s}_{enc}, pk^{u,s}_{sig}$ *with* s
7: s executes:
8: $(pk^{s,u}_{sig}, sk^{s,u}_{sig}) \leftarrow \mathcal{G}_{sig}()$
9: s *shares* $pk^{s,u}_{sig}$ *with* s
10: // Both u and s have $sk^{u,s}_{enc}, pk^{u,s}_{sig}, pk^{s,u}_{sig}$
11: **return** $pk^{u,s}_{sig}, pk^{s,u}_{sig}, sk^{u,s}_{enc}$
12: **end procedure**

Formule1 : Generating a compound identity

3. Communication Workflow

Step 1: Node Authentication & Identity Verification

Each node is required to authenticate before it can access or share data:

1. Public/Private Key Generation:

Nodes generate asymmetric key pairs (RSA-4096 or ECC-256). Public keys are stored on the blockchain.

2. Decentralized Identity Verification (DID-based Authentication):

Nodes register on a blockchain-based identity system using Decentralized Identifiers (DIDs). Authentication is done via Zero-Knowledge Proofs (ZKP) to prevent exposure of sensitive data.

Step 2: Secure Data Request & Access Authorization

1. A data requester submits a signed access request to a smart contract.

2. The smart contract verifies the requester's:

   - Identity (DID Verification)
   - Access Permissions
   - Reputation Score (Proof of Trustworthiness)

3. If authorized, the contract logs the request on the blockchain and grants access.

Step 3: Data Encryption & Key Management

The requested data is encrypted using AES-256 before transmission. The encryption key is split using Shamir's Secret Sharing and distributed across multiple blockchain nodes Only authorized users can reconstruct the key and decrypt the data.

Step 4: Secure Data Transfer & Integrity Verification

The data provider encrypts the file and generates a hash (SHA-256) of the encrypted content. The data is transmitted using peer-to-peer (P2P) channels. The requester validates the data hash before decrypting the file.

Step 5: Data Audit & Compliance Logging

Every access request and transaction is logged on the blockchain, ensuring auditability and compliance. A Merkle Tree-based system ensures data consistency without exposing actual content. Users can verify who accessed data and when, ensuring accountability.

Protocol 2 Permissions check against the blockchain

procedure CHECKPOLICY(pk^k_{sig}, x_p)
  $s \leftarrow 0$
  $a_{policy} = \mathcal{H}(pk^k_{sig})$
  if $L[a_{policy}] \neq \emptyset$ **then**
    $pk^{u,s}_{sig}, pk^{s,u}_{sig}, POLICY_{u,s} \leftarrow Parse(L[a_{policy}])$
    if $pk^k_{sig} = pk^{u,s}_{sig}$ **or**
($pk^k_{sig} = pk^{s,u}_{sig}$ **and** $x_p \in POLICY_{u,s}$) **then**
      $s \leftarrow 1$
    end if
  end if
  return s
end procedure

Formule 2 : Permissions check against the blockchain

4. Consensus Mechanism

DSDTP supports:

Proof of Authority (PoA):

- Used for private/enterprise blockchains. Validators are pre-approved entities ensuring efficiency.

Proof of Stake (PoS):

- Used for public blockchains. Nodes stake tokens to become validators.

Protocol 3 Access Control Protocol

procedure HANDLEACCESSTX(pk^k_{sig}, m)
  $s \leftarrow 0$
  $pk^{u,s}_{sig}, pk^{s,u}_{sig}, POLICY_{u,s} = Parse(m)$
  if $pk^k_{sig} = pk^{u,s}_{sig}$ **then**
    $L[\mathcal{H}(pk^k_{sig})] = m$
    $s \leftarrow 1$
  end if
  return s
end procedure

Formule 3 : Access Control Protocol

Protocol 4 Storing or Loading Data

1: **procedure** HANDLEDATATX(pk^k_{sig}, m)
2: $c, x_p, rw = Parse(m)$
3: **if** $CheckPolicy(pk^k_{sig}, x_p) =$ `True` **then**
4: $pk^{u,s}_{sig}, pk^{s,u}_{sig}, POLICY_{u,s} \leftarrow Parse(L[\mathcal{H}(pk^{u,s}_{sig})])$
5: $a_{x_p} = \mathcal{H}(pk^{u,s}_{sig} \parallel x_p)$
6: **if** $rw = 0$ **then** ▷ rw=0 for write, 1 for read
7: $h_c = \mathcal{H}(c)$
8: $L[a_{x_p}] \leftarrow L[a_{x_p}] \cup h_c$
9: (DHT) $ds[h_c] \leftarrow c$
10: **return** h_c
11: **else if** $c \in L[a_{x_p}]$ **then**
12: (DHT) **return** $ds[h_c]$
13: **end if**
14: **end if**
15: **return** $\emptyset$
16: **end procedure**

Formule 4 : Storing or Loading Data

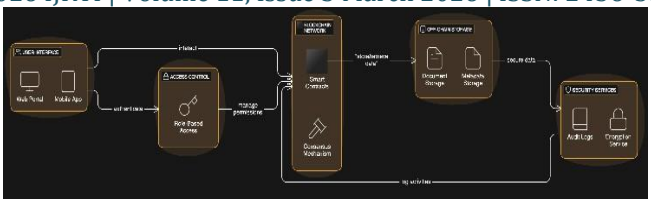

Figure 1. Architecture Diagram

Figure 2. SHA1 vs SHA-256

V. PROPOSED SYSTEM

The proposed system includes the transition of legal and crime management in blockchain te chnology. By using blockchain, decentralized storage is deployed to ensure redundancy and resilience to node errors. Each block is interna lly encrypted for improved data security. Chec king data integrity is facilitated by the associat ion of transparent hash codes with each block, allowing operation detection. Smart contracts developed using Solidity Programming regul ate document management processes and prov ide transparent, immutable transaction books.

Improved security: Blockchain encryption and decentralization provide robust protection aga inst operations and unauthorized access.

Transparency: The immutable ledger ensures t ransparency and accountability in document management.

Resilience: Distributed memory reduces the ri sk of data loss due to server failure or cyberatt acks.

Reliability: The nature associated with the ope ration of a blockchain conveys trust in the reli ability of legal documents.

Efficiency: Smart contracts automate docume nt management tasks, reduce management ove rhead costs, and tighten processes.

System Architecture Blockchain-based Evacht sys tems were developed using comprehensive layers and components to provide secure, decentralized management and legal document storage. The syst em ensures data integrity, accessibility and transpa rency, while maintaining high safety standards an d scalability. It guards the architecture and detaile d breakdown of each component. This detailed arc hitecture provides a comprehensive, scalable and s ecure design for blockchain
based Evacht. By using intelligent contracts, role-based access, and offchain storage, Evahat achiev es a high level of safety

1. UI Layer:

   Manage user roles and access rights for se cure document interaction. Document Upl oad interface: Enables users to safely uplo ad legal documents. A central surface wher e users can manage and view documents a nd related activities.

2. API Gateway

   Considering exposure to large, common da ta records in the model, it is necessary to fi ne-tune it with smaller, domain-specific da tasets to improve performance within the t arget domain and at the same time reduce general distortion. This involves sending k nowledge from preformed models, but par ameters are gradually adapted to learn new domain-specific patterns without distortin

g previously trained data. The fine tune pr ocess uses reduced learning rates to contro l model convergence. This preserves over-adjustment and generalization skills

- LLDM=Ez0,c,ϵ,t‖ϵ-ϵθzt,t,c‖22

Where:

- z0 is the latent representation of input data.
- c is the conditioning signal (e.g., CLIP embeddings).

3. Debiasing Techniques:

Data Scaling is used to improve model exposu re compared to underestimated features, objec ts, and scenarios within the training dataset. B y generating random transformations such as r otations, color jitter, and images with rare pro perties, the model outweighs all specific attrib utes and is less likely to learn a more balanced representation of different subjects.During tra ining, bias correction algorithms are impleme nted to recognize and reduce trends towards di storted output. This includes including fairnes s data and fairness restrictions to ensure balan ced predictions for other sensitive categories i nformed by fairness-conscious AI frameworks .

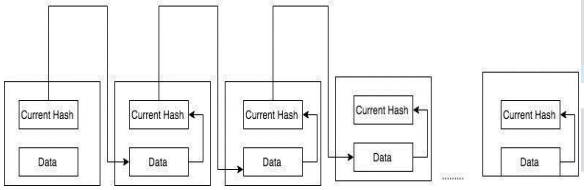

Figure 3. Blockchain Implementation

Prompt Engineering and Control Samples: Th e diversityof the generated editions is improve d by ratio engineering, and input requests are created to promote the model tocreate a larger starting area. Controlled sampling techniques such as temperature scaling and classification guidance allow for the generation of images to capture different characteristics, improving th e inclusiveness of your initial presentation.

- pθ(xt-1|xt)=N(xt-1;μθ(xt,t),Σθ(xt,t))

Where:

- μθxt,t is the predicted mean.
- Σθ(xt,t)) is the variance, often simplified for efficiency

4. Integration of CLIP for Enhanced Semantic Alignment:

A multimodal open source model, Clip is u sed to ensue that the generated images mat ch the demands of text by drawing languag e and image features in a shared embedded space. By including Clip Embedding, a st able diffusion model can help you better u nderstand the context and nuance of input requests, reduce misunderstanding, and re duce unclear potential distortions in textua l descriptions.

LCLIP=-cos(ftext(c),fimage(x))

Where:

- ftext(c),fimage(x) are CLIP embeddings for text and images

5. Variational Autoencoder (VAE) for Improved Image Quality:

The VAE component of the stable diffusion m odel enables realistic and consistent image ge neration by improving latent representation. B y coding the input data in compressed latent s pace and reconstructing it during the diffusion process, VAE improves quality and sharpness -generated images.In this project, the VAE is f inely tuned next to the other models, ensuring consistent, high quality image generation in th e target domain. This also helps reduce artifact s that can affect image realism..

- LVAE=Ex~p(x)[‖x-D(E(x)+ϵ)‖2]+K L(q(z|x)‖p(z))

Where:

- E(·)encodes data into latent space.
- D(·)decodes latent vectors to reconstruct the input.

6. Evaluation and Bias Analysis:

Quantitative Metrics: Evaluate image quality and diversity using standard metrics such as Inception Score (IS) and Cheeky Inception Distance (FID).

These metrics evaluate how the generated images match the actual image distribution exactly and di splay the realism and variation of cost.Awareness and Equity Assessment: To assess the effectivenes s of the committee's technology, preloads are dete cted using algorithms to evaluate generated image s of overrepresented or underestimated properties. Quantify the degree of distortion using metrics su ch as demographic parity and equal opportunity. T his step includes cross-validation, which validates the images generated against the training dataset, and analysis of balanced presentations on demogr aphic data.

- Equal Opportunity:

  $\Delta opportunity = |P(y^=1|y=1,d1) - P(y^= 1|y=1,d2)|$

- Demographic Parity:

  $\Delta parity = |P(y^=1|d1) - P(y^=1|d2)|$

VI. RESULT

As discussed earlier The following section presents the outputs of login and adding of legal documents by the admin. The generated outputs are shown in figure 1,2,3,4:

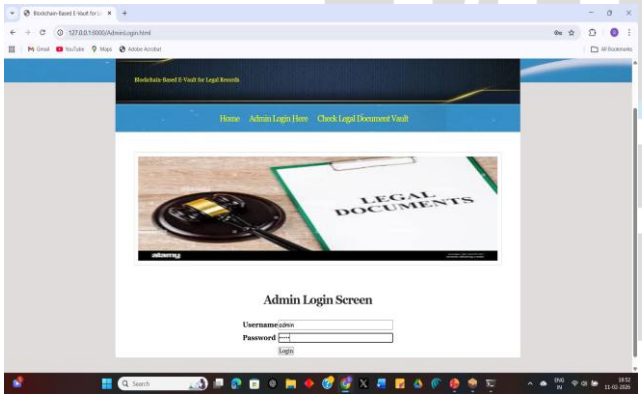

Figure 1.Admin login page

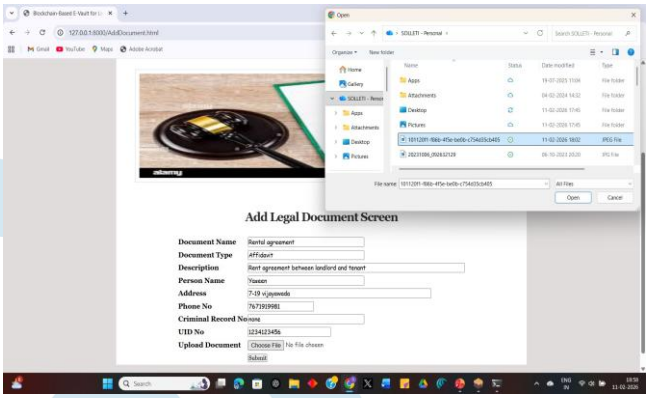

Figure 2.Document upload page

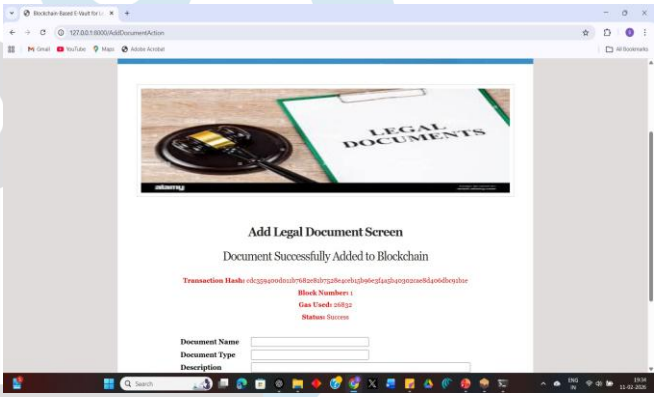

Figure 3 Document converted to Hash code

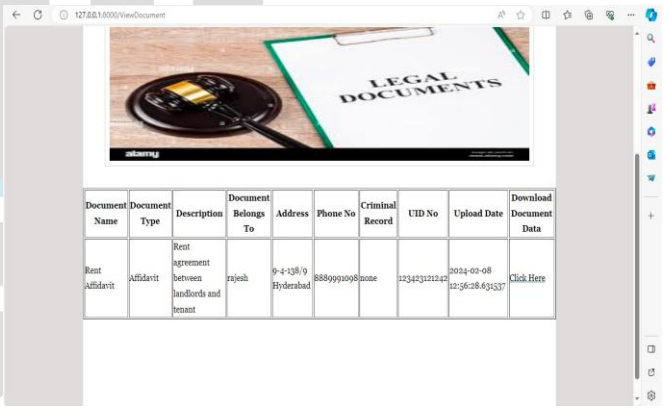

Figure 4 View list of document

As a result of the screen above, you will receive th e type of details for the rental document, upload it to the relevant document data, then click the Subu te button to save the blockchain data and save the output to the screen above. When returned to the b lockchain storage, the transaction hash code is usu ally displayed, but all details are displayed and all guides are displayed. All details will be displayed. In the above editions, the hash code and block nu mber can be viewed as the core edition. Next, clic k on the "View Documents" link to display all sav ed document editions of the blockchain on the scr een above in the right area. You can download rela ted data. Then, once you register, regular users ca

n view all available legal documents. However, alt hough we do not provide document data for the do cument, we cannot download related data. On the next screen, regular users can search for legal doc uments

VII. Conclusion

In summary, the transition to legal and criminal do cument management in blockchain technology pro vides a robust solution to tackling the weaknesses of central servers. Blockchain-specific security fu nctions and distributed storage reduce the risk of d ocument modifications and unauthorized access. By eliminating dependencies on a single point of control, it improves data integrity and reliability, r educing the likelihood of corruption or cyberattac ks. This transition ensures transparency, trust and unchanging records, protecting the integrity of co urt cases and the confidence in the protection of c onfidential information from manipulation or loss.

A. Futuer work

Future improvements could be focused on improv ing blockchain protocols to optimize speed and sc alability and ensure seamless integration into exist ing legal systems. More intelligent contracts can b e developed to automate processes such as contrac t execution, dispute resolution, increased efficienc y, and reduced costs. Implementing advanced encr yption technology can enhance data protection an d at the same time improve AI control solutions fo r document analysis and verification. Furthermore , by investigating interoperability between differe nt blockchain networks, it is easier to pass inform ation and receive security at the same time. Contin uous research and development efforts are crucial to harnessing the full potential of blockchain tech nology in legal document management and promo ting a safe and transparent future.

VIII. References

[1] Lone, A.H. (2017). "Forensic-chain: Ethereum blockchain-based digital forensics chain of custody."

[2] Al Omar, A., Rahman, S., Basu, A., & Kiyomoto, S. (2017). "MediBchain: A Blockchain-Based Privacy Preserving Platform for Healthcare Data."

[3] Liang, X., Shetty, S., ToshLaurent, D., & Njilla, L. (2017). "ProvChain: A BlockchainBased Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability."

[4] Ramachandran, A., & Kantarcioglu, M. (2018). "SmartProvenance: A Distributed, Blockchain Based DataProvenance System."

[5] Ølnes, S., Ubacht, J., & Janssen, M. (2017). "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing."

[6] Dinh, T.T.A., Liu, R., Zhang, M., & Wang, J. (2017). "Untangling Blockchain: A Data Processing View of Blockchain Systems."

[7] Setiadi, I., Kistijantoro, A.I., & Miyaji, A. (2015). "Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems."

[8] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). "MedRec: Using Blockchain for Medical Data Access and Permission Management."

[9] Иванов, С., Розберг, Е., Иванов, И., & Ягубов, Г. (2016). "Анализ результатов лечения больных хроническим панкреатитом."

[10] Guy Zyskind, Oz Nathan, and Alex 'Sandy' Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data, "2015

[11] Javad Zarrin, Hao Wen Phang, Lakshmi Babu Saheer, Bahram Zarrin, Blockchain for decentralization of internet: prospects, trends, and challenges, Cluster Computing 2021

[12] Morteza Alizadeh, Karl Andersson, and Olov Schelen, Efficient Decentralized Data Storage Based on Public Blockchain and IPFS.

[13] Saqib Ali†, Guojun Wang, Bebo White, Roger Leslie Cottrell, A Blockchain-based Decentralized Data Storage and Access Framework for PingER,2018

[14] XuhuiChen, JinlongJi, ChangqingLuo, WeixianLiao, PanLi, When Machine Learning Meets Blockchain: A Decentralized, Privacy-preserving and Secure Design

[15] Vishal Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Informatics Journal 2019

[16] Srivastava, Gautam; Dwivedi, Ashutosh Dhar; Singh, Rajani, Crypto-democracy A Decentralized Voting Scheme using Blockchain Technology P. Esser *et*

[17] *Yogesh M. Gajmal and R. Udayakumar, Blockchain-Based Access Control and Data Sharing Mechanism in Cloud Decentralized Storage System, Journal of Web Engineering,*

Vol. 20 5

[18] HANAN E. ALHAZMI 1,2, FATHY E. EASSA 1, AND SUHELAH M. SANDOKJI1, Towards Big Data Security Framework by Leveraging Fragmentation and Blockchain Technology,2021

[19] Sarita Simaiya, Umesh Kumar Lilhore, Sanjeev Kumar Sharma, Kamali Gupta, and Vidhu Baggan, Blockchain

[20] Jamal N. Al-Karaki, Amjad Gawanmeh, Meryeme Ayachek, Ashraf Mashaleh, DASS-CARE: A

[21] Decentralized, Accessible, Scalable, and Secure Healthcare.