Blockchain Network based Decentralized Applications for Healthcare Sector

B. Santhanakrishnan
School of Computing Science and Engineering,
Vellore Institute of Technology,
Chennai, 600127, Tamilnadu, India.
santhanakrishnan.b2020@vitstudent.ac.in,

Amit Kumar Tyagi[0000-0003-2657-8700]
School of Computing Science and Engineering,
Vellore Institute of Technology,
Chennai, 600127, Tamilnadu, India.
amitkrtyagi025@gmail.com

Terrance Frederick Fernandez [0000-0002-7317-3362]
Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, TN, INDIA
frederick@pec.edu

Abstract. Distributed computing is a well-known concept in the contemporary era. Every big technological company/firm runs their applications on servers distributed across the world. It compliments multiple benefits, including yet not limited to rapid response times to clients and better reliability. But, distributed the server may be, or it is still under the control of a centralized entity, i.e., the company spearheading the servers. Decentralized applications, abbreviated as DApps, aims to counteract this drawback. The server-side code of DApps are stored and executed upon a decentralized peer-to-peer network, like an Ethereum blockchain. This way, DApps maintain all the advantages of a distributed computing system while presenting several added benefits.

Keywords: Blockchain, DApps, Ethereum, Decentralization, Healthcare.

I. INTRODUCTION

With the advent of emerging technologies such as Artificial Intelligence and the Internet of Things, healthcare is undergoing a massive transformation. Over the past years, Information Technology has undergone a massive upscaling transformation. Healthcare however, did not catch up. Naturally, this rendered various undesirable effects such as knowledge-based exploitation, and data mining without proper consent and law abidance [1]. Another issue with conventional systems is the lack of interoperability. "Healthcare providers" - a group which can be taken to mean doctors, researchers, or nurses for the rest of this study, manage their data on the hospitals own database. If a patient goes to another hospital, the hospital may only get limited data about the medical history - only what is present in the patient's medical card. If an individual wants to receive web or telephony-based consultation, they may find it hard to without there being a convenient way to consensually share their data with the healthcare provider. Therefore, we must come up with a way to combat this by adapting the healthcare industry to modern information standards. The topic of this study, DApps (Decentralized Applications) fit this in this work paper perfectly, as we shall see.

A. Objective of this work

Establish a proof-of-concept for a mathematically secured data model for the healthcare industry, which ideally provides a trustless data store for patients, hospital records, and anything of the like.

B. Blockchain - Introduction

The first use-case for the blockchain was in cryptocurrency. However, substantial interest has grown in the usage of the blockchain in other contexts. For the purposes of this paper, the blockchain can be dumbed down and viewed as an immutable data store, which enables interactions between two entities without the requirement of any trusted third party. This is in stark contrast to current systems where the private/public hospitals maintaining health records act as an implicitly trusted third party. But, is this really an advantage? Can't one argue that having a trusted third party would mean that disputes would be easily resolvable, among other things? To answer this question, we need to touch upon the cryptographic base the blockchain stands upon. The blockchain runs on a backbone of four principles:

- Decentralization: Any computing resources that are required for the hosting of the DApps is shared among all the nodes in the network, this means that no one node has all the pieces to the puzzle, and manipulating the network is much harder than on a centralized network.
- Trustless-ness: In the world of centralized computing, and centralized data storage, every participant in the system depends upon the righteousness of the central authority to manage their data in an ethical and legal way. In a decentralized system such as the blockchain, each and every participant has a full copy of the data, called a "blockchain ledger", and therefore if a single node goes rogue, or goes offline due to a mishap, it won't affect the system.
- Security: With its public key infrastructure, blockchain ensures that there is no way to access any record in it unauthorized, and even effects due to vulnerabilities in physical interfaces are limited to just that node. This also ensures data integrity.
- Privacy: Any two parties can interact on the blockchain network, anonymously, with limited fee, and privately, behind a cryptographically secured wall.

978-1-6654-8035-2/22/$31.00 ©2022 IEEE

C. Security in the Blockchain

The blockchain uses public key cryptography for its security. In public key cryptography, each interacting entity maintains a public key, and a private key. In order for two parties to send messages to each other, the sender must encrypt their message using a combination of their private key and the receiver's public key, creating a key-pair. The keys are configured so that the receiver can decrypt the message with their private key (no one else can do so), and this decryption will also confirm that the sender is indeed who they claim to be. It is not possible to "invert" this process, and find out the private key of the sender. This is due to mathematical concepts that lie outside the scope of this paper, which can be referenced in the original paper on RSA Cryptography [2] - the most widely used form of public key cryptography.

II. ARCHITECTURE

Blockchain-based healthcare systems must provide medical history, maintain medical records, and ensure that patients have full control over who gains access to their data. Most important, it should be able to achieve all this while keeping the door open for a potential increase in user-base. Vertical scalability must also be achievable, as the number of peers in a network may be limited in some settings.

Choice of blockchain platform is also important. One consideration is the legal issues which arise out of some countries' laws being averse to cryptocurrency. This would imply the need to use a specialized blockchain platform which does not issue digital coins, and is permissions-based - therefore not requiring expensive computations or "mining", which is against rules in many countries, due to its high energy requirements. However, this limitation is expected to be a temporary one, as more and more countries are starting to include blockchain technology considerations in their laws. So, we shall freely utilise popular public blockchains such as the Ethereum network, and lay a roadmap for future projects.

With this in mind, we can present an architecture as follows:
Every patient registering on the peer-to-peer network received their own copy of the immutable blockchain ledger, and will add their information to it in the form of blocks. Each block can contain a massive amount of information, transactional, health-related, bloodline-related, etc. The consensus and sequence validity of these blocks are uniformly maintained by each node in the network by virtue of smart contracts [3], which are, to put it simply, a programmatic way to ensure each node in the network is in sync with a common 'plan' on maintaining data integrity.

From a software perspective, we can assume four entities to be involved in the system - an Administrator, the doctors, researchers, and patients, interacting with the following modules - registration, record maintenance, record sharing, record retrieval and record verification, each of which is detailed below.

A. Registration

This module deals with patients, doctors or researchers registering themselves to utilize the software system. Registration of an entity must be protected by multiple middleware. This middleware must ensure that

- if the entity is a healthcare provider, they must be licensed, and certified
- every entity has registered themselves with the underlying blockchain network properly.

B. Record Maintenance

This module deals with the updation/deletion of records from the database. This module is only available to individuals who have registered themselves, and have also been granted permission to access the records by the owner of the record -- be it a patient, or a healthcare provider.

C. Record sharing

This module deals with the use-case of a healthcare provider requiring to view a patient's past records. This will require the owner of the record, typically a patient, authorizing the viewer, typically a healthcare provider to gain access to a part, or the whole of their record. Unauthorized accesses should be logged and inspected.

D. Record retrieval

Just like maintenance, entities will require authorization in order to retrieve any records from the database. However, an unauthorized access pipeline will be set up to facilitate moving all the records - without being able to access them, in the event of infrastructure change, or other assorted reasons.

E. Record Verification

Apart from the blockchain's inbuilt transaction verification, sanity checks related to the health data needs to be performed. This will include checking their criminal history, and their transaction history on the blockchain. Healthcare providers will also be "rated" via feedback from patients, so this will also be checked.

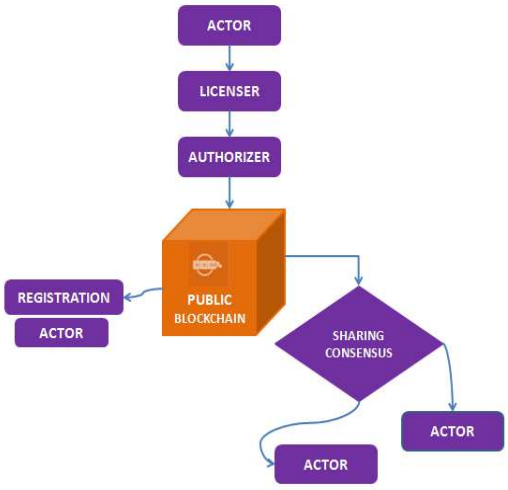

Fig. 1. Basic illustration of the Blockchain architecture.

III. BUILDING TRUST

The very purpose of this study is to establish a structure which ensures that patients can gain 100% trust in healthcare workers, and securely transfer healthcare information. To solidify this into the core of the application, we shall establish trust specifications in a formal manner.:

- License Issuers: Similar to SSL certificate issuers [4] of the present-day internet, an authoritative issuer will decide whether or not a healthcare provider will be licensed to operate.
- Authorizers: They will ensure that each time a healthcare provider fetches data from the blockchain ledger, they are authorized by the owner of the record to do so. They shall also be the entity that can revoke a license.
- Evaluation and feedback: Once the treatment by an authenticated and authorized healthcare provider is

complete, the patient may provide feedback to the system. It is important that this feedback be anonymous, and this can be built through a simple one-time authentication process. Future patients may use this information as a trust factor for the healthcare provider.

- Judiciary: The administration of the whole system; This entity decides when to revoke a license, based on patient feedback, and when to abolish patients from the network, or in general, any arbitrary node. Since this is a human component, its detailed discussion has been neglected in this study. The only note made of it pertains to how the system will incorporate input from the judiciary. This can be done with any run-of-the-mill user and group permissions system.

Note that in this work, simply the phrase "authorized" may be taken to mean both 'authenticated" and "authorized" for the sake of brevity.

IV. REFACTORED ARCHITECTURE

With the barebones of the trust model, and the software modules established, we can decide upon a second iteration of the architecture. The patient is nothing more than a "feedback provider" as far as the software is concerned. The doctors and researchers are nothing more than "licensees" as far as the software is concerned. The administrators, Licensers, and authorizers are nothing more than "license providers", as far as the software is concerned. We can represent this at a high level pictorially as shown in figure 2.

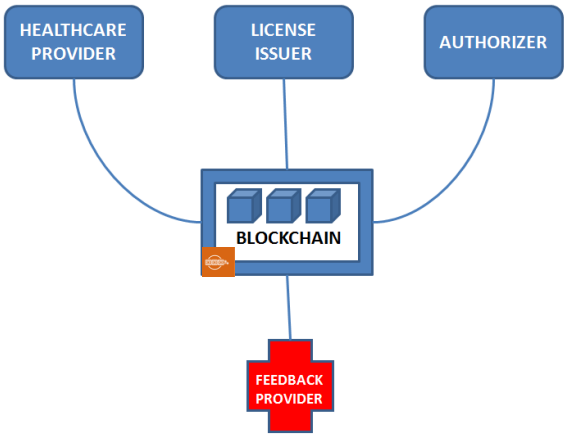

Fig. 2. A high-level view of the Proposed Architecture

In this manner, the system is guaranteed to capture the trust of patients, and put in place a system to handle the whole pipeline of data - patient data - healthcare provider data - feedback logging - licensing. This trust relationship is the essence of the whole system. To ensure that this trust is maintained, human authoritative bodies must be set up, preferably elected. However, this is akin to an implementation detail. The actual data security is mathematically audited due to the blockchain, and does not require dependence on any authority. Beyond that, the human element, again, is out of the scope of this study.

V. IMPLEMENTATION

DApps are built on a decentralized network, which for the purpose of this study, shall be assumed to be the most popular one - the Ethereum network. The business logic of the application runs on the blockchain's nodes, and the source code is written in the solidity [1] language using "smart contracts". A major advantage in DApps is that their frontend code, and the UI can be written in standard languages such as JavaScript, HTML and CSS, as the frontend will simply run on the client's web browser.

Regarding the infrastructure, an Ethereum DApp consists of the user's web browser, an Ethereum container running an Ethereum API for a suitable programming language, and the backend "smart contract" running on all the nodes - notice the lack of requirement for backend infrastructure (on-premise, or on a centralized cloud)!

For this study, the execution environment shall be assumed to be the JavaScript VM, Node.js, with web3.jsbeing the Ethereum API. The testing framework used will be Truffle. A walkthrough of the skeleton for the proposed implementation has been provided below. For demonstration purposes, we shall take upon the implementation of the registration module.

In tabular form, figure 3 shows what a block containing registration information would look like.

Type	License issuer	Authorizer	Valid until	Hash	Unix Timestamp
Healthcare provider	0x8973...jCh293	0x7fhF84...82Fs2	1697394600000	0x784bhgF...xhr5	1634455468593
Patient	0xduf2F...D284u	0xhudy42F...895	1697394600000	0xjht38748...dh5X	1634455478953

Fig. 3. The data structure to be used for the registration model

A smart contract corresponding to the table in **Figure 3** has been modelled in the Solidity programming language (which is used on the Ethereum network) in the source code below

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.4.21;

contract Registration {
enumentity_type
{
Patient,
Healthcare_Provider,
}
struct data{
entity_type type;
bytes32 issuer_hash;
bytes32 authorizer_hash;
uint256 valid_until;
bytes32 trHash
uint256 timestamp;
}

data storedData;

function set(data x) public {
storedData = x;
}

function get() public view returns (data) {
return storedData;
}
}
```

We also present a small front-end application that will process this data, a snippet of which has been provided in source code below. It is written with the front-end javascript framework - React.js

```
import { useEffect, useState } from "react";
import SimpleStorageContract from
"./contracts/SimpleStorage.json";
```

```
  import getWeb3 from "./getWeb3";

  import "./App.css";

  export default function app() {
  const [state, setState] = useState({
  data: {},
  web3: null,
  accounts: null,
  contract: null,
  });
  useEffect(async () => {
  try {
  const web3 = await getWeb3();
  const accounts = await web3.eth.getAccounts();
  const networkId = await web3.eth.net.getId();
  const deployedNetwork =
SimpleStorageContract.networks[networkId];
  const instance = new web3.eth.Contract(
  SimpleStorageContract.abi,
  deployedNetwork&&deployedNetwork.address
  );
  setState({ web3, accounts, contract: instance });
  example();
  } catch (error) {
  alert(
  `Failed to load web3, accounts, or contract. Check
the console for details.`
  );
  console.error(error);
  }
  }, [state]);

  const example = async () => {
  const { accounts, contract } = state;

  await contract.methods
  .set({
  type: "patient",
  issuer_hash: "0xuyd7837483hjdhjf27f232",
  authorizer_hash: "0xhdh2FS24fhw43s3F4x",
  valid_until: Date.now() + Date(2024, 08, 31),
  trHash: "0xuiH23fIie420S19839fhq205d32",
  timestamp: Date.now(),
  })
  .send({ from: accounts[0] });

  const response = await
contract.methods.get().call();

  // Update state with the result.
  setState({ data: response });
  };

  if (!state.web3) {
  return <div>Loading Web3, accounts, and
contract...</div>;
  }
  return (
  <div className="App">
  <h2>Smart Contract Example</h2>
  <div>The stored value is: {state.data}</div>
  </div>
  );
  }
```

Note that the full source code of the proposed application will be made available on the author's git repository, accomplished with a developer's documentation.

VI. ADHERENCE TO LAWS AND REGULATIONS

A. Introduction

Health data is sensitive, and thus requires privacy. Controlling access to it properly is essential, and this must be done in accordance with laws and regulations such as the GDPR [5], and health data laws such as the HIPAA [6], and data laws of each nation the system is operating in. The right balance must be maintained between adhering to the laws, and adhering to the core values of the system - consensual, and transparent data sharing.Whether or not the general compliance requirements of the GDPR [5] are strictly adhered to by the blockchain remains up for debate in most computational forums [7]. As and when a consensus is reached on this issue, this study may have to be updated. For the time being however, all future studies instigated on this topic must include a full compliance report, or suggest a change in the requirements with the respective committees.

B. Privacy Requirements

Below listed are the privacy requirements for such a system to adhere to most laws and regulations.

- **Non-Identifiability**: The identity of any entity involved in the system must be treated as confidential. Purely with information within the blockchain, it must not be possible to link the real-life identity of an entity with their presence on the blockchain. This will be kept in accordance with the clauses present in the GDPR [5]. Any analytics generated should, at a minimum, make it impossible to reverse-engineer the patient's identity from the data.
- **Data access:** A patient, or any entity owning data stored on the blockchain, must explicitly give a say-so before any other entity gains access to their data.

VII. SOFTWARE REQUIREMENTS

Several systems requirements like functional and non-functional can be discussed as:

A. Functional Requirements

Functional requirements for Blockchain network can be:

a) **Closure of trust**: Any trust-building verification a healthcare provider gives to a patient must be fully based on information from the blockchain. No other information must be required.

b) **Transparency**: The data must be hosted on a public blockchain. These may have a fee to operate on, which must be taken care of.

c) **Governance**: There must be an API which human elements, such as governance entities, which provide licenses, and other certifications discussed can access [8].

7.2 Non-Functional Requirements

Non functional requirements for Blockchain network can be:

Security

- All entity interactions must be cryptographically protected, so as to avoid fraudulent interactions.
- The integrity of the interaction logs must be maintained, by storing it on the blockchain, where it is possible to prove the immutability of the data.

Availability

- **Addition and modification of governance entities.** The governance API discussed above must accommodate the same.
- **Performance.** The number of blockchain transactions must be minimized so as to reduce power consumption. This is discussed further in the drawbacks section.

- **Durability**. The DApps must be configured such that any mishap from human or other natural elements involved can be easily reversed, and the application restored to a previously known clean state.

VIII. DRAWBACKS OF BLOCKCHAIN

Many disadvantages of using Blockchain network for building DApps can be discussed here as:

- It is a major change from traditional approaches to data management. Even large companies are struggling to integrate it into their workflows.
- High initial capital. The huge amount of processing power combined with the hype around the technology make it an impossible investment for smaller companies.
- Although it can handle small data like identities, the blockchain begins to falter when larger data has to be stored.
- Power consumption. Blockchain technology requires an immense amount of computing power, which will be especially pronounced when it is used at the scale of healthcare. With current technology, this leads to an extreme amount of energy usage, which could cause environmental concerns.

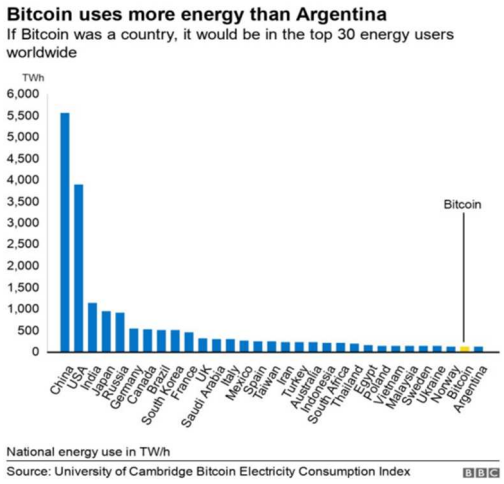

Fig. 4 Comparing the energy consumption of Bitcoin, with whole countries!

The University of Cambridge Bitcoin Electricity Consumption Index, published results which affirmed that energy consumption due to bitcoin mining *alone* consumed more energy than the whole country of Argentina [9] as shown in figure 4**.** Israa Abu-elezz et al. conducted a study [10] which outlined 8 threats of blockchain influence in the healthcare sector, the most significant of which are - scalability issues, transaction costs, interoperability issues, and high energy consumption, which is usually coupled with slow processing.

IX. ASSESSMENT AND OTHER RELATED WORK

For assessing the quality of a blockchain-based healthcare system, the following metrics are to be considered.

- *Programming Language*: The programming language the source code of the DApp uses must be turing complete. Many presently-utilized languages are built solely for the purpose of monetary transactions. Healthcare DApps need to utilize a wide range of features that would require a Turing complete programming language in order to be implemented reliably and efficiently. Ethereum is one such platform.
- *Interoperability*: Let's not forget, one of the core values this study is built upon is open-ness and free-ness. All this would go out of the window if various healthcare platforms start to lock in their users, similar to centralized tech giants of today. To avoid this, every DApp must use a standardized data structure to store patient information, and it must be exportable to common formats, and in a manner that the owner of the data is able to easily transfer it to another platform, if they so wish. It is imperative that this exists in both a structural sense, and a semantic sense. Every effort must be made to ensure seamless interoperability between all competing platforms.
- *Cost-effectiveness:* For building a scalable DApp, we must be able to, eventually, bring it to a cost-effective equilibrium, which is better than existing non-blockchain-based technologies.
- *Interests:* The primary interest behind any design/technical/architectural decision taken must be the patients.
- *Compliance:* The regulations discussed above - GDPR and HIPAA must be adhered to by the system.

Related Works and Adoption

Aside from proof-of-concepts - which are present in abundance, there are multiple practical healthcare DApps in their infancy. One open-source project "Blockchain for healthcare" available at https://github.com/sarveshraj/blockchain-for-healthcare presents a healthcare DApp, that also takes care of drug sales, and pharmaceutical services. Another open-source project HealthBuddy, available at https://github.com/rsd511/HealthBuddy-DApp presents a similar architecture, with chemists being considered as an entity. Many open-source frameworks are being developed for making the adoption of a blockchain-based healthcare system more feasible, providing a reliable base for settings with little financial room for experimentation.

In the last, many attempts towards implementation of Blockchain in Healthcare or other sectors are discussed in [12-22] by Tyagi eta. al. The researchers can refer these articles to know possible uses of emerging technologies in the smart era/ for their future research work.

X. CONCLUSION AND FUTURE SCOPE

This study showed a proof of concept of blockchain's potential influence on the healthcare industry, it's numerous benefits and at least for now, equally numbered drawbacks. However, with advancements in energy efficiency, and research advancements culling some of the drawbacks stated apriori, the benefits of blockchain could far outweigh the drawbacks. The healthcare community can then strive towards adopting the technology, and training its members on the technical aspects of the adoption. Software companies can extend this model and design a continuously integrated software solution.

Blockchain, or potentially, another similar technology more specialised for healthcare, will improve the data sharing in healthcare immensely, no doubt. The assurance of immutability, traceability, transparency and decentralization it provides is a huge boon to the healthcare industry, plagued for the past decade by information scandals, frauds and data exploitation, majorly owing to the centralized nature of corporate healthcare [11, 14 and 15].

From a software perspective, potential improvements include

a) *Incorporation of more entities:* As mentioned earlier, many DApps also include chemists, and other kinds of healthcare professionals as entities. This could be incorporated into the architecture presented here. However, this is not completely necessary, as pharmaceuticals, and emergency work, pose a lot of out-of-the-book problems, which will require a human element in order to be rectified. For example, automating the process of assigning emergency workers might not be the best idea, as the information on the actual urgency of the requirement is lost, and in many cases, it is better to leave this to human elements.

b) *More specifications for the functional requirements:* Although it is hard to gauge now, many unaccounted-for aspects of the software system will become evident once healthcare DApps become prevalent on the large scale. These must be promptly included. These could pertain to scalability issues, or interoperability with existing government systems.

c) *Accounting for cultural differences:* Healthcare is a universal requirement. However, delivering healthcare services smoothly requires taking the local culture into account. Different cultures respond differently to various healthcare models. So, even though the main goal is to have a unified and robust healthcare system, there will be some amount of deviation in each country, based on the local culture.

REFERENCES

[1] George, S. L., & Buyse, M. (2015). Data fraud in clinical trials. *Clinical investigation*, *5*(2), 161–173. https://doi.org/10.4155/cli.14.116

[2] *R.L. Rivest, A. Shamir, and L. Adleman*: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Volume 21, Issue 2, Feb. 1978, pp 120–126, https://doi.org/10.1145/359340.359342

[3] Khan, S.N., Loukil, F., Ghedira-Guegan, C. *et al.* Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Netw. Appl.* 14, 2901–2925 (2021). https://doi.org/10.1007/s12083-021-01127-0

[4] S. F. Al-Janabi and A. K. Obaid, "Development of Certificate Authority services for web applications," *2012 International Conference on Future Communication Networks*, 2012, pp. 135-140, doi: 10.1109/ICFCN.2012.6206857.

[5] The GDPR enactment, https://ec.europa.eu/info/law/law-topic/data-protection_en

[6] https://www.cdc.gov/phlp/publications/topic/hipaa.html

[7] https://www.ncbi.nlm.nih.gov/books/NBK9573/

[8] Colin Alexander Boyd, Trust and Transparency in Digital Society Through Blockchain Technology, Available at: https://app.cristin.no/projects/show.jsf?id=2041854

[9] Olivier Rikken, Marijn Janssen and ZenlinKwee, Governance challenges of blockchain and decentralized autonomous organizations. Information Polity, 24 (4), 397-41, DOI 10.3233/IP-190154

[10] The University of Cambridge Bitcoin Electricity Consumption Index, https://cbeci.org/index

[11] Siddharth M. Nair, Varsha Ramesh and Amit Kumar Tyagi, Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications, Book: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles, 2021, Pages: 14, DOI: 10.4018/978-1-7998-3295-9.ch012

[12] Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, ArildFaxvaag, Blockchain in healthcare and health sciences—A scoping review, International Journal of Medical Informatics. Vol. 134, IJMI, Elsevier, 2020, https://doi.org/10.1016/j.ijmedinf.2019.104040

[13] Amit Kumar Tyagi, Aswathy S U, G Aghila, N Sreenath "AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN, Volume 2, Pages 175-183, October 2021.

[14] Amit Kumar Tyagi, Meghna Mannoj Nair, Deep Learning for Clinical and Health Informatics, in the book "Computational Analysis and Deep Learning for Medical Care: Principles, Methods, and Applications", 28 July 2021, DOI: https://doi.org/10.1002/9781119785750.ch5

[15] Amit Kumar Tyagi, Dr. Meenu Gupta, Aswathy SU, ChetanyaVed, "Healthcare Solutions for Smart Era: An Useful Explanation from User's Perspective", in the Book "Recent Trends in Blockchain for Information Systems Security and Privacy", CRC Press, 2021.

[16] Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security 2020, Vol. 15 Issue 1, p1-16. 16p.

[17] M. M. Nair, A. K. Tyagi and N. Sreenath, "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-7, doi: 10.1109/ICCCI50826.2021.9402498.

[18] Madhav A.V.S., Tyagi A.K. (2022) The World with Future Technologies (Post-COVID-19): Open Issues, Challenges, and the Road Ahead. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_22

[19] B. Gudeti, S. Mishra, S. Malik, T. F. Fernandez, A. K. Tyagi and S. Kumari, "A Novel Approach to Predict Chronic Kidney Disease using Machine Learning Algorithms," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2020, pp. 1630-1635, doi: 10.1109/ICECA49313.2020.9297392.

[20] Tyagi A.K., Fernandez T.F., Mishra S., Kumari S. (2021) Intelligent Automation Systems at the Core of Industry 4.0. In: Abraham A., Piuri V., Gandhi N., Siarry P., Kaklauskas A., Madureira A. (eds) Intelligent Systems Design and Applications. ISDA 2020. Advances in Intelligent Systems and Computing, vol 1351. Springer, Cham. https://doi.org/10.1007/978-3-030-71187-0_1

[21] Tibrewal I., Srivastava M., Tyagi A.K. (2022) Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi A.K., Abraham A., Kaklauskas A. (eds) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore. https://doi.org/10.1007/978-981-16-6542-4_1

[22] Mishra S., Tyagi A.K. (2022) The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artificial Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-030-87059-1_4