International Journal of Intelligent Networks 2 (2021) 175–183

Contents lists available at ScienceDirect

International Journal of Intelligent Networks

journal homepage: www.keaipublishing.com/en/journals/international-journal-of-intelligent-networks

AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology

Amit Kumar Tyagi [a,b,*], S.U. Aswathy [c], G. Aghila [d], N. Sreenath [e]

[a] Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India
[b] School of Computer Science and Engineering,Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India
[c] Department of Computer Science and Engineering, Jyothi Engineering College, Thrissur, Kerala, 679531, India
[d] Department of Computer Science and Engineering, National Institute of Technology, Karaikal, Puducherry, India
[e] Department of Computer Science and Engineering, Pondicherry Engineering College, Pudcuherry, India

ARTICLE INFO

Keywords:
Medical cyber physical system
Cyber security
Blockchain technology
Security
Privacy
Innovation
Cryptography

ABSTRACT

The enhancement (in the past decade) in electronics devices/technology, a rise in most of the accidents concerning security and surveillance intruding the private lives of the users question the existing systems being used to combat this challenge wherein, the third-parties gather and handle large amounts of individual details. As part of the constant evolution of the cyber physical system architecture, one of the goals of our system is to reduce the latency time for enrollment of new information. Generally, the efficiency and benefit of a Cyber Physical Systems (CPS) depends heavily on interconnection of individual devices or nodes. Exchange of data and information relevant to an overall task or functionality is the key to many applications such as smart grids, smart cities, and many others. Trustworthiness of data is needed to make such systems (especially in MCPS systems) successful. To be able to fulfill policies to guarantee the safety of all entities within a Medical Cyber Physical Systems (MCPS) and to provide security measures to enforce these cryptographic solutions have to be embedded. This paper describes a decentralized e-healthcare application framework for personal data management that ensures that users own and access their data. This work proposes a novel mechanism to secure Medical Cyber Physical Systems (MCPS), i.e., as an automated access-control manager (including building trust in a third party). This work also integrates some features in security building blocks in ultra-small devices to provide essential properties to secure embedded systems.

1. Introduction – cyber physical system

Bitcoin has introduced a new technology to provide security with a higher degree of trust using decentralized and distributed concepts [1]. Today the same technology (i.e., Blockchain technology) is used in various applications like creating new cryptocurrency, finance or smart contract, auditable computing, etc. To overcome lack of security issues in the available cyber physical system, Organizations/Government may use Blockchain as a game changer. In general, there are several types of cyber physical systems (build with the combination of physical and cyber space), which are included as: Industrial Control System CPS, Smart Grid CPS, Medical CPS, Smart Cars/Automotive CPS, Household CPS, Aerospace CPS, Defense CPS.

These CPSs are built through interconnection of Internet of Things (IoTs) together, i.e., on a large scale. High levels of security and stringent measures to prevent unnecessary breaches of data can be acquired by using digitally verified birth certificates which cannot be manipulated or time stamped and is inaccessible to all people. Blockchain technology tries to solve above raised issues but we need to ask one question here: "What challenges do we currently face in our transaction networks?" Let's consider the case wherein the absence of the essential element of trust leads to friction. This can be easily solved in the presence of Blockchain, as the shared ledger it implements helps in enhancing the transparency of transactions, thus improving trust. If business agreements or make delays (in providing of services), smart contracts may be the solution. The aim in this present study is to determine "how Blockchain can help overcome specific challenges"? As discussed, the first widely known and discussed Blockchain was the Bitcoin Blockchain [1], and it serves as the de-facto

* Corresponding author. Centre for Advanced Data Science, Vellore Institute of Technology, Chennai, 600127, Tamilnadu, India.
E-mail addresses: amitkrtyagi025@gmail.com (A.K. Tyagi), aswathy.su@gmail.com (S.U. Aswathy), aghilaa@gmail.com (G. Aghila), nsreenath@pec.edu (N. Sreenath).

https://doi.org/10.1016/j.ijin.2021.09.007
Received 26 June 2021; Received in revised form 24 August 2021; Accepted 25 September 2021

example of how Blockchain systems can work. In a Blockchain block, each block contains the data present in the block and a header which given a description of the data held in each block.

In fact, Blockchain is a simple, sequentially arranged set of transactions which are time-stamped along with a number of output addresses which are 160 bit long. Bitcoin Blockchain is the grandfather of public Blockchains, or is also called as 'permission less' Blockchains, i.e., anyone can write data into it by running any free software without signing up. Bitcoin can be considered as an electronic form of currency which makes use of Blockchain technique [1]. The distributed form of database built on the foundations of Blockchain is often referred to as Blockchain 2.0 and it includes smart properties and smart contracts (the former consists of assets controlled by Blockchain ownership, while the latter include software which control the smart properties). Currently, the concept Blockchain 3.0 has been put forth and it also seems to be a viable option [2,3]. We can define Blockchain technology as: "Blockchain Technology (BT) is a distributed, shared, encrypted, irretrievable, and inalterable database system along with a consent mechanism, permitting communicative exchanges between the users" [4–6]. Note that amount of data (in cyber physical systems) is rapidly increasing, which is a critical issue to handle/to provide security to entire database [7–9].

While we extract and implement the profits of a society completely dependent on data, there's a pressing concern to address the issue of the users' privacy. A majority of public and private centralized organizations possess massive amounts of personal and intricate details. People have hardly any control over this data and in the past few years, the media has started the coverage of all possible controversial incidents pertaining to privacy, all across the globe. Note that here SECURITY expands to S-Sensible, E-Efficient in work, C-Claver, U-Understanding, R-Regular, I-Intelligent, T-Talent, Y-Yield management/Young. Fig. 1 in Ref. [10] provides a difference between centralized, decentralized, and distributed structure. Today's CPS is creating a huge amount of data at the server side which is difficult to manage. In our work, we use an IoT-enabled Blockchain as a shared ledger to record every activity of every user/-transaction as they communicate in a system. Recording of every transaction/document (being done in network) called smart contract. Autonomous upgrades of the smart contracts can be augmented with the help of IoT systems/devices in order to uproot the foreign trade invested on IoT linked Blockchain systems. The major advantages of using Blockchain Technology include:

- Increased flexibility and transparency of shipment process, enhancing the system.
- Growth in faith and trust while all transactions are logged and maintained.
- Increase in precision and accuracy to cut through IoT involvement.
- Participants are permitted to augment and boost up business through IoT implications.
- Futuristic targets and goals for "freight autonomy".

Using Blockchain technology in our work, we can provide higher security and a sufficient level of trust to world users against stored data in a central database. With respect to storage of data and its' apt management, plausible damage from external attacks and intrusions can be avoided. Moreover, due to the fact that openness is a key feature of Blockchain, it helps in the provision of data flexibility and transparency on application to data and details which require data disclosure. Due to such strong and capable reasons, it's widely used in a number of fields like finance, IT, IoTs, etc.

1.1. Medical cyber physical system

With the advent of integrated cyber and physical techniques, healthcare in the digital world has proven to be an outburst of success. This brings our close attention towards different types of medical devices which brings about a physical impact on the client. These are either conveniently placed within the patient's body or are worn by them and are respectively called as IMDs or Wearable Devices. These usually come attached with wireless mechanisms in order to facilitate networking with other similar devices, physicians, programmers, etc., for plenty of needs [7,8]. Healthcare devices (MCPS) can be classified into stationary medical devices, embedded medical devices, portable medical devices and devices for portable health monitoring. Notice that the first sensor pill (aripiprazole tablets with a sensor) inside it will check whether the patient has swallowed it. This pill sensor sends data to a wearable patch, and the patch itself passes the data to the web application on the handset. In the near future, this device could be a game changer for chronic illnesses, mental health disorders, and many diseases. The Internet of Things (IoT) is a network of wearable computers embedded with devices, electronics, sensors, actuators and networks that allow data to be connected and exchanged by the wearable user [7,9,11].

One of the most critical elements of human life has been health insurance, which leads to a major increase in large-scale health data [12]. To ease the diagnosis and recovery process, healthcare providers are now accepting wearable technologies focused on the Internet of Things (IoT). In recent years, billions of sensors, computers, and cars have been linked to the Internet for people or businesses to exchange knowledge on the road. One such technology that is common today for the treatment and care of patients is Remote Patient Monitoring (RPM). In RPM, via cyberspace, i.e., through the internet, the doctor takes care of his/her patient remotely. Note that RPM is part of the Physical Medical Cyber Structure, which incorporates both physical and cyber spaces for treating patients. However, these applications (IoT-based Cloud Systems) often face major privacy threats and security concerns surrounding data transfer and recording of data transactions. Such questions about the security of medical records and privacy can arise from a delay in the advancement of treatment, even endangering the patient's life. Security and privacy considerations are present today in every application. Notice that many IoT security and privacy problems were addressed by Tyagi et al. [13–16].

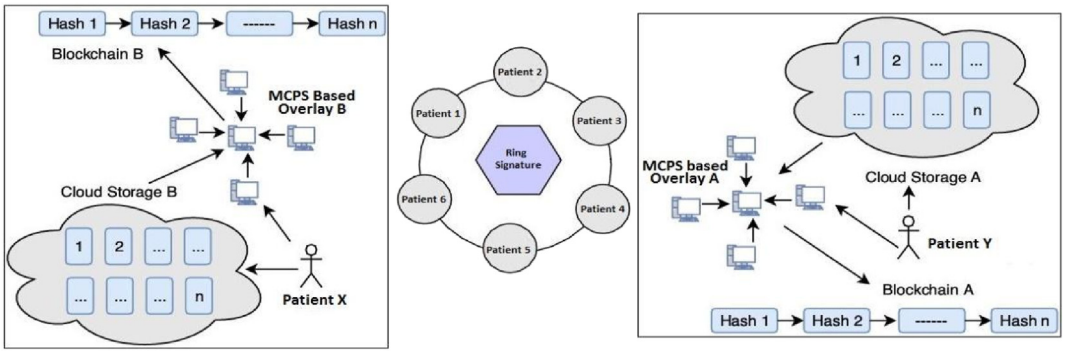

Fig. 1. MCPS based Overlay Network.

In this work, we propose the use of a blockchain in an accessible, effective manner to provide stable management and analysis of big data in healthcare. Note that blockchains are costly for storage, require large bandwidth and extra processing resources, and are not entirely sufficient for most resource-constrained IoT devices intended for smart cities or large networks. Through the use of Blockchain through an overlay network in our work, we are trying to solve the above discussed problems of using Blockchain combining with IoT devices. We are proposing a new architecture with modified Blockchain models appropriate for IoT devices which focus on distributed nature and other additional privacy and protection features of the network.

In our work, privacy and defense properties are focused on advanced cryptographic principles. The technologies provided here cater to a Blockchain-based network render IoT application data and transfers data safely and anonymously. Readers are encouraged to read [10] to learn more about Blockchain technology. Blockchain and its integration with artificial intelligence and the internet of things can be found in Refs. [17, 18]. It is to be observed that Consensus Function is a mechanism that urges a majority of the Blockchain nodes to come into an agreement on a certain message along with ensuring that the recent blocks have been correctly added to the existing chain, and assure that event like “fork attack” or other malicious intrusions do not occur. Here, Proof of Work (PoW) is useful on a public Blockchain, such as the one used for Bitcoin, but it demands for large amounts of power, and electricity, thus leading to the jingle of loose coins in the server ‘s pockets. Such expensive measures are to be avoided and hence, using Consensus Mechanism, Blockchain helps in the propagation of trust and ensures that the users remain anonymous. Monero, Dash, ZCASH are examples of Blockchain implementations with the essence of anonymity. On the contrary, Zero Knowledge Proof (ZKP), is a worthwhile example for assuring that no information will be let out. This concept, merged with the technique of Blockchain can do wonders by reassuring the closed atmosphere of information regarding the transaction procedure. It is indeed a proof method which sufficiently acknowledges completeness, inconveniency, and Zero Knowledge. Hence in summary, Blockchain technology preserves privacy of users during making transactions by providing anonymity among all users. Apart from anonymity, there are six major keys to Blockchain Technology i.e., Decentralized character, Flexibility and Openness, Automation, Unchangeable, and Anonymity. Note that factors which make Blockchain technology popular and useful/a revolutionary technology are: SHA256 Hash Function, Public Key Cryptography, Distributed Ledger & Peer to Peer Network, Proof of Work and Incentives for Validation.

We discuss all the enhancements in/of cloud, with the Internet of things for CPS (which received several challenges). These challenges or problems or serious issues need to be solved in future research. From a comprehensive systems perspective, the CPS system needs to be analyzed very carefully and thoroughly. Irrespective of the number of plausible surveys and analyses of CPS systems, most of these don't have a fully-fledged working model for assuring privacy (when CPS systems are collecting data from multiple services; neither do they take into account sufficiently the systems perspective). For example, majority of the observations in Ref. [8] calls for the presence of an access model. Our work elucidates the security perspectives of the MCPS and throws light on the issues concerning the existing system including those of replay attacks with the help of biometrics, profile-tracking of individuals, etc. We put forward our analysis of these problems and propose solutions. Hence in section 2, we will discuss security and privacy issues raised in MCPS system (its working architecture). Then in section 3, we discuss our objectives. Further, a detailed description of our proposed work will be discussed in section 4. Simulation work will be discussed with various simulation parameters and metrics in section 5. Then, we explain how Blockchain could become a critical resource in trusted computing in section 6 through our platform and a discussion of potential technology improvements. Finally, in section 7, we will conclude our proposed work with various potential changes/work in brief.

1.2. Blockchain technology in big data

Blockchain is indeed an organized and systematized sequence which stores details similar to that of a distributed database. Each block includes a header and some content, wherein the header consists of hash values from the preceding and current ones. The data is then searched in the database using index methods. Irrespective of whether the block holds the hash value of the succeeding block or not, it's often added, making it easier to collectively join the blockchain with big data. There are mainly two possible combinations: data management and data analytics. The former refers to Blockchain storing larger amounts of data and ensuring its originality. Consider the case of Blockchain being used to record the details of patients, this ensures that data remains unalterable and secure. The latter however deals with using Blockchain transactions for Big Data analysis. For example, the trading routines of the users can be retrieved and clients are able to judge the mannerisms of the possible partners Transactions on Blockchain could be used for big data analytics when it comes to data analytics. Consider the case of consumer trading habits and mannerisms being extracted. The clients can easily reciprocate the mannerisms of the peers as per the research survey. As discussed in Ref. [10], technical steps have been used/implemented to improve Blockchain ‘s stability, such as proof of work, functional Byzantine fault tolerance, delegated stake proof and stack proof. Therefore, on a Blockchain network (due to the use of a consensus function/ledger mechanism), practically everything of value can be monitored and exchanged, minimizing risk and reducing costs for all concerned.

2. Related work

A number of researchers and scholars who seem to be experts in this field have attempted to solve the issues concerning privacy and security from a legal and legislative perspective [4]. Open PDS is a recently created model/architecture putting forward the automated deployment of a PDS which consists of mechanisms involved for the return of computations. Fig. 2 provides the evolution and popularity of Blockchain in the past decade (since its evolution). Majority of the top-class companies in this industry decided to get working with their very own proprietary validation software building their foundation on OAuth protocol [4], which involves centralized trusted committee members. From the viewpoint of security and safety, researchers have introduced a number of techniques and methodologies in order to target the safety issues pertaining to personal data and content. The method of data anonymization aims towards securing personal and private information and details. K-Anonymity is a profound and highly used technique of unknown datasets and it calls for the sensitive and intricate data pertaining to each individual record which is often confused with at least k-1 of the other records [19]. L-diversity is an extended version of k-anonymity and it ensures that the intricate data has a varying set of values to be modelled [20]. T-closeness is another such example which studies spread of intricate data [21]. Recently, we have proved that datasets can be anonymized easily and how they can be de-anonymized with the support of these methods [19–22]. A few of the other methods for securing the privacy of data includes differential-privacy. This is a technique that calculates data and imparts noise to the process of computing before data sharing [23] and other methods of encryption. In fact, Fully Homomorphic Encryption (FHE) schemes permit computations to take place over the encoded data, however, they seem to be currently inefficient and slow to be used on a large scale. That is the main reason as to why novel classes of reliable systems are being developed. Blockchain is also used for securing several other projects and applications (collectively referred to as *Bitcoin 2.0*). Fig. 2in Ref. [10] discusses the evolution of Blockchain Technology since its birth year. Hence, this section discusses related work to Medical cyber physical systems and Blockchain technology. Now, the next section will discuss the problem of security and privacy in MCPS with examples.

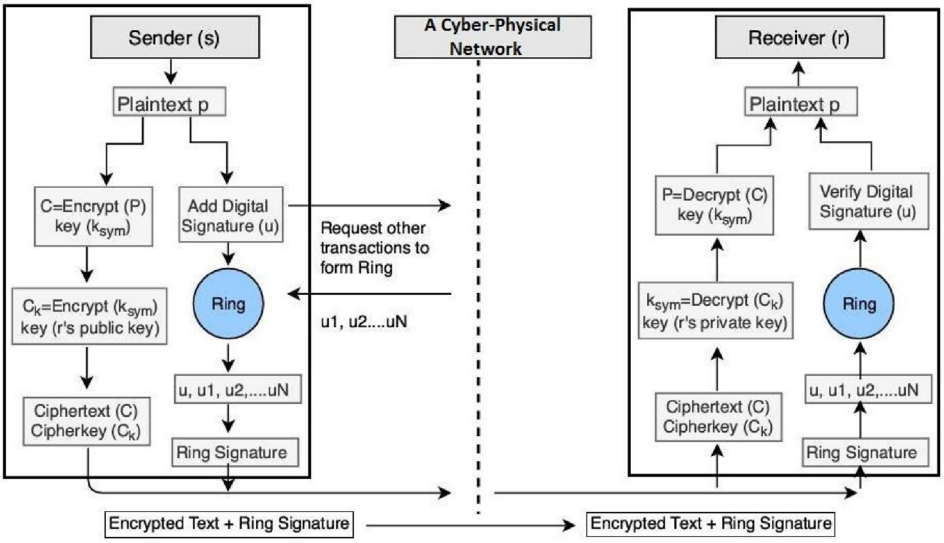

Fig. 2. Proposed system.

3. The Security and privacy problem with cyber physical systems

In recent years, the emergence of IoT and wearable technologies have improved the quality of patients care through remote patient control. It also allows doctors to help more people. Remote Patient Management (RPM) [8] provides patient monitoring and treatment outside the conventional healthcare environment (at home, for instance). First, the inherent ease of patient care is allowed. Patients should be linked with health providers as needed. It also reduces hospital costs and raises the quality of service. This is the key reason why healthcare workers are looking for means to deliver RPM to the masses. Wearable devices capture patient health data and send it to hospitals or medical facilities to facilitate health monitoring, disease identification, and treatment. Note that wearable healthcare devices are smart electronic devices with microcontrollers that can be inserted as accessories in clothes or mounted on the body. They are unobtrusive, user-friendly, and connected to advanced features including computer-installed wireless data transfer, real-time feedback, and alert systems. These devices will give healthcare providers vital information, such as blood pressure, blood glucose levels and breathing patterns, etc.

Secure and reliable transmitting of medical data is the primary concern in RPM networks. For hackers, healthcare information is a lucrative target and the main motivation for healthcare practitioners is to protect protected patient information (PHI). The biggest focus for cybercriminals has been healthcare. In the last decade, for instance, cyber-attacks on medical devices or health data have become more frequent.

However, blockchain technology in its original form is not enough of a solution [24]. Several challenges [5,11,25] we faced during applying Blockchain to the IoT and explanation how we recovered that.

- Decentralization – using a MCPS network as overlay
- Authentication of data – using lightweight digital signature
- Scalability-not proof of operation, but instead of a single block chain, broke our overlay network into several clusters, since a single blockchain is not responsible for all nodes. We distribute the nodes over many clusters instead. The dispersed life of the network and other additional security properties are the foundation of our model.
- Encrypted data blocks for data storage-Cloud-Stored. We store all transactions in separate blocks and create a combined hash of each block using the Merkle Tree and transfer it to the distributed network. It is quick to recognize any improvements in cloud data in this manner. The storage also retains decentralization of such regions in this manner.
- Authentication: We use the lightweight Ring structure [26] along with digital signatures for authentication. The signature of the ring requires the data to be anonymously signed by a signer, i.e. the signature is blended with other groups (named ring) and no one knows which member has signed the letter (except the real signer)
- Data security: Medical equipment or health records must be secure and they should not be changed by hackers. To save data from hackers, we use a double encryption scheme. In this case, double encryption does not apply to the use of two keys to encrypt the same data, but to the encryption of the data and the encryption of the key used to encrypt the data. By way of lightweight ARX algorithms, we encrypt the data and then encrypt the key using the recipient's public key. We often use the Diffie-Hellman key exchange technique for the transmission of public keys, but it is almost difficult for an intruder to get the keys.

To guarantee that the integrity of the data is preserved, the data is not changed, lost or damaged. Access to data should be regulated by patients, but they should not be able to alter it themselves. Reliable and open medical information should be available across disciplinary borders [27, 28].

Hence, Medical CPS involves modern medical technologies and issues which consist of complex embedded systems which are facilitated with communication services and are capable of supervising the control and physical aspects of a patients' body. For example, proton therapy machines, electro-anatomical mapping, bio-compatible and implantable devices, and robotic prosthetics. Each time these devices end up faulty or broken, they end up negatively affecting the patients' health. Hence, the validation and certification of their proper functioning is of prime importance, though it is a herculean task to accomplish. For example, in 2010, Stuxnet was a bug that had adversely affected Iran and illicitly interfered in its' Nuclear Facilities [29]. Furthermore, in 2010, a few of the attackers had combined a software tool named ‘Car Shark’ which is likely to kill remote car engines and to a certain extent even switch off the brakes in order to prevent the car from stopping or send any false readings to the Electronic Control Units (ECUs). On the whole, these days, different security vulnerabilities are discovered in numerous CPSs including those of power grid, smart transportation and healthcare systems, etc.

In fact, we have also acknowledged the privacy issues and concerns faced when implementing third-party services. Our main focus is on

mobile frameworks which mainly make use of applications for installation purposes and these gather high resolution data of individuals which doesn't have any particular detailing or control to it. Through the analysis we carried out, we have realized that the services are indeed honest but yet, they're curious. It's to be observed that the very same system can be made use of for different privacy issues including those of sharing the medical history of patients for scientific purposes, etc. Putting it in a nutshell, our system is capable of securing data from the below mentioned privacy concerns:

- Data Ownership: The users are in complete control and ownership of their individual data. Under normal circumstances, the system identifies the users as the controllers of the data and other services with validated and authorized permissions.
- Data Transparency and Auditability: Every user has the flexibility and procured control over the details being gathered about him/her along with the way they're being accessed.
- Fine-grained Access Control: One of the prime concerns pertaining to mobile applications is the requirement for a number of permissions to be granted following a sign-up.

And these allowances are granted indefinitely. However, in our framework or architecture, the user is free to modify the granted permissions at any instance of time along with revoking access to the details collected earlier.

One of the major applications of this mechanism is to modify and improvise the current allowances in the mobile applications. The user-interface mostly would remain the same, even though the access control norms and regulations can be changed as they are stored in Blockchain.

Hence, this section discusses security and privacy problems in medical cyber physical systems. In further sections, we will discuss several issues related to the cyber physical system in brief.

4. Security and privacy issues in a cyber physical system

Cyber physical systems provide individuals with some advantages, but are not free from privacy and security concerns. As the interaction between the physical and computer systems grows, the physical systems are becoming more and more vulnerable to cyber system security vulnerabilities [30]. During different stages of the CPS (or its operating process), many security and privacy problems can occur. Security and privacy issues can arise during CPS (in a centralized database) collection, transmission and storage. These things have to be meticulously taken care of. Otherwise, a number of serious problems can affect users/individuals. Biometric data are often used by CPS systems for unique identification of people and authentication. However, biometric systems can become susceptible to possible attacks. Any of these flaws in security include the following:

a) Biometric Capture Systems vulnerabilities: CPSs offer various services to many users. Other businesses are awarded contracts to take care of the key aspects of the CPS system. Therefore, these businesses can affect or be prone to biometric/personal information from users.
b) Private Actors and Data Leakage: A big opportunity for data leakage is stored/collected data. Many private staff are involved in the entire sequence of registration and data generation processes through the CPS communication system. Therefore, it is important to determine the honesty and responsibility of the people/users involved in the activities.
c) Cryptographic algorithms: CPS systems are covered by the security of commercial networks and by cryptographic products bought from various suppliers. Because of the usage of these systems, the potential for data loss, disruption or eavesdropping, monitoring or hacking of confidential and private data increases exponentially.
d) Infrastructure failures: Infrastructure failures due to power failure or server failure which result in sensitive personal information being lost. Natural calamities can also cause any portion of the protected infrastructure of the CPS (or a government) to break down, leading to data damage and loss.
e) Access Control: Another essential security measure that should be taken care of is access control. It is important to properly identify and track access rights that govern who can access any service (from electronic devices) and the applications/devices that manage/generate such data. Any access control information penetration and alteration can lead to devastating consequences.
f) Human error: Human beings involved in the entire CPS/setting relation process may trigger problems either accidently or maliciously. Agents may leave the device unlocked, and transport storage tapes may be lost.
g) Security and Privacy Issues in a Centralized CPS Database: The CIDR database is a centralized database containing all-in-one information about an individual. It is still feasible to snoop and hack into this database. The development of a broad centralized database and the real-time transfer of sensitive data over networks raise important operational and security issues. The entire identification scheme would fail if the database crashes. Designers can have high redundancy by using parallel systems and mirrors to ensure reliability and availability in order to circumvent this problem. This can, however, increase security problems and the privacy of biometric data. There are also major risks associated with the transmission of biometric data over computer networks, where, even without any detection, it can be tapped, copied, and changed.

In addition to the above debate, health data is highly confidential and information sharing will increase the risk of disclosure. So far, many emerging data sharing systems use a centralized architecture that involves centralized trust. Blockchain technology might and could very well be the solution for data privacy and security. The inability to remove or alter block details renders the Blockchain the healthcare system's most appropriate technology. However, the adoption of Blockchain in the IoT context is not straightforward and entails many challenges, such as high PoW addressing processing power requirements, poor scalability and long network transaction confirmation latency. We are proposing a novel Blockchain model and removing the PoW concept to make it acceptable for IoT applications. We offer a lightweight ring signature scheme for the protection of privacy that is ideal for anonymous transactions by authentic users for anonymity and user identification. A lightweight digital signature assures that the information has not been changed, as if it were covered by a tamper-proof seal which, if the contents were changed, would be broken. In Ref. [31], an introduction was made to the techniques for using Blockchain to provide evidence in clinical trials with pre-specified endpoints. Using a clinical trial procedure where result swapping had previously been documented, Irving and Holden empirically validated such a method. It acknowledged the use of Blockchain as a low-cost auditing tool that can be independently tested and confirmed the reliability of research studies. In our [11,26]-influenced model, we use lightweight digital signature schemes.

In addition, a ring signature [26] enables a signer to anonymously sign a message. The signature is mixed with another group (named ring) and nobody knows which member has signed the message (except the real signer). To make it more appropriate for Blockchain and IoT, we don't use strong operations such as pairing and exponentiation in the ring signature. Using lightweight encryption algorithms (ARX cyphers) and public encryption methods, we also use double data encryption. Double encryption here means we first use symmetric key encryption to encrypt the details and then use a public key to encrypt the symmetric key itself. Notice that in this work, we do not encrypt the same data twice with different keys. Using three simple arithmetic operations, ARX is a family of cryptographic algorithms: modular addition, bitwise rotation and exclusive-OR. In our work, both in industry and academia, its success is

the reason for choosing ARX. The ARX cypher has won a great deal of recognition and publicity in recent years. Moreover, we use the Diffie-Hellman key exchange method to securely exchange cryptographic keys over a public channel. Lightweight approaches suitable for compact IoT devices would guarantee customer data protection, safety and confidentiality by using all of these strategies together. This section therefore briefly addresses many problems related to the cyber-physical climate and the solution to the raised problem (proposed in our work). Now, our proposed work will be discussed in detail in the next section.

5. Proposed solution

The current Blockchain Technology is very similar to that of a characteristic technology which assures user anonymity. If this technique is combined with the cloud computation process, Blockchain can be effortlessly boosted up to a comfortable and convenient service which ensures supreme security and privacy. Each time some information or content is created and is being passed on for storage purposes, then these details are protected with the help of Blockchain techniques. Furthermore, along with securing information, trust and loyalty is easily enhanced amid clients and organizations.

We begin by overlaying our system's complete overview. There are three cases that make up our scheme, as seen in Fig. 1,: cell phone users eager to download We start with our device overview. As outlined in Ref. [17], cell phone users who are involved in downloading and utilizing the application are the three entities comprising our system; services, suppliers of this application who need to process individual information for organizational and commercial purposes (e.g. targeted advertising, customized service); and nodes, instances assigned to maintain the Blockchain and a shared private key It is to be noted that we can store the data in Blockchain each time the user remains anonymous/unknown and check it accordingly. The framework was developed as follows: two separate modes of processing can be obtained through Blockchain: T_{data} that is used for storing and extracting data; T_{access} that is useful for management supervision. Data which is gathered up on a phone is encoded with distributed encryption key and is forwarded to the Blockchain using a T_{data} transaction, routing it off to an off-Blockchain key--value store, by logging certain pointers to the public ledger (the pointer is the SHA-256 hash of the data). The service and data can equivalently query the details and information related to the corresponding pointers with the help of T_{data}. The blockchain then validates and authorizes the digital signature which is owned by either the client or the service. In the end, the permissions to retrieve and meddle with data are cross-verified by issuing T_{access} processing with a novel set of permissions. Creation of a web-based dashboard which permits an overlook of a persons' data and their power to change permissions is insignificant and is equivalent to developing Coinbase for Bitcoin, etc. Since the occurrence of transactions are based on the value of time of a mobile device, the confirmation regarding its security completely depends on the integrity and accuracy of time stamps which are created in a particular mobile. As discussed earlier, Blockchain is a massive technique which permits all its users, not only to log ledgers consisting of transactional data, but to also update them and to maintain it consolidated. With the exponential enhancement in Internet and encoding, technology has made it possible to validate and cross-check the doings of members/clients and keep a sharp eye on them, as well as their third-party members. Blockchain is also instilled with broker-free features and is thus, efficient enough to waive out needless fees using P2P (peer to peer) processing without approval from third-parties.

5.1. CPS authentication architecture

Note that our system (proposed approach) consists of five MCPS components, including cloud storage, overlay network, healthcare providers, smart contracts, and healthcare wearable IoT devices for patients.

- Cloud storage: We use cloud storage servers to store patient data instead of storing IoT healthcare data over Blockchain. User information is organized into similar blocks connected to a single block number by cloud storage. This cloud is connected to overlay networks [11], and the cloud service sends the hash of the data blocks to the overlay network until the data is stored in a block. Merkle Tree [2] is used to measure the hash of the data in a single block. When the root hash of the new block is approved by the overlay network, the new hash with the prior hash value is added and the chain ‘s new hash is created. We may not require any third-party trust in such situations, since any changes in data will easily be traceable.
- In our overlay network model, the network consists of individual nodes and they need a valid certificate to prove that they are certified. It is possible to upload or validate such a certificate prior to setting up an account on the network. Unless authorized, he/she would be able to digitally sign the data/transaction over the network. We group these individual nodes in the form of multiple clusters to increase network scalability and avoid network delays. Each cluster has one cluster head that looks after the nodes' public keys. Any node linked to any cluster, in the event of a delay, can adjust the cluster at any time. The nodes added to a cluster can alter the head of the cluster as well. The cluster head holds the public keys of the applicants (healthcare providers) who are entitled to access the data of a specific patient and the public keys of the applicants (patients) who are eligible to access them. Notice that if any node's digital signature or public key is not verified using the key mechanism when verifying data, the cluster will not broadcast the data in its cluster but will transfer the transaction to other cluster heads. It is also the responsibility of cluster heads to store the hash stored in the cloud of the data block. A cluster head can independently decide whether to maintain the latest hash of the data block or not. It will transmit it to all clusters when a new hash is inserted by a cluster chief. Other clusters use the previous chain's hash value to verify the current block as well. Each cluster head maintains a trust rating for the other cluster heads based on the Beta Credibility Scheme [32,33] in order to track distributed network trust. We suggest that readers refer to the following papers for further explanations of overlay networks [34,35]. Readers are also urged to refer to Ref. [32] for more information about religion
- Insurance firms or patients are appointed by healthcare providers to conduct medical tests or to offer medical services.
- Smart contracts authorize any IoT system that is applied to form agreements when the conditions are fulfilled in this work. Consider specifying the criteria for the maximum and lowest level of blood pressure in the patient. The smart contract will send an alert message to the approved person or healthcare provider when readings are taken from the wearable device that do not adhere to the specified range, and store the suspicious data in the cloud so that the patient's blood pressure readings can be collected later by healthcare providers if appropriate. If appropriate, healthcare providers will later take blood pressure levels from the patient as well.
- Both health data from the patient will be obtained by the IoT system. Heartbeats, sleeping conditions, or walking distance, to name a few, can be such data. Patients themselves are the owners of their medical records and are responsible for some other agency, such as insurance agencies or healthcare providers, authorizing, refusing or revoking data access. He or she will exchange confidential health records with the desired doctor if the patient needs medical attention. Further access to the clinic, hospital provider or health insurance plan may be refused by the patient before the procedure is finished.

As discussed above cyber physical systems are a combination of physical and cyber space [8]. Here, cyberspace requires a new cyber security mechanism to protect a database against cyber vulnerabilities. A Physical space is where systems directly are accessible to human beings. This process also needs to be secured by physical security, hardware security, etc. To secure a cyber-physical system, we need to protect an IoT

ecosystem smartly and efficiently. Internet of Things (IoT) Security at different Layers can be provided as: IoT Perception Layer Security, IoT Network Layer Security, IoT Transport Layer Security and IoT Application Layer Security.

In our model, we used symmetric and asymmetric cryptographic techniques, i.e., ARX encryption algorithm (used to encrypt data for Blockchain) and digital signature (for authentication purposes), digital ring signature (to provide anonymity to signer and maintaining correctness of signature during sharing of messages) and Diffie - Hellman key exchange (to exchange public key separately, for providing more security). As discussed above, due to resource limitations on IoT devices, the implementation of normal digital signatures is not sufficient. Note that our proposed system is primarily steadfast to protecting the network from multiple attacks instead of defending discrete nodes. In a case where a default node is located inside the network, we can block it automatically. SPECK (the latest use of ARX cypher) is a Feistel-like structure family of lightweight block cyphers in which each block is divided into two branches and both branches are updated in each round. The overview of our proposed work is given in detail in Figs. 1 and 2. In addition, many 1, 2, 3 and 4 algorithms are used for encrypting, key sharing, decrypting, and signature authentication.

5.1.1. *Explanation of cryptographic algorithms used in our work*

Small contracts using Blockchain technologies provide that the ownership of the asset is passed to a scrap dealer who is allowed to dispose of the vehicle under another smart contract. With the Blockchain network, CPSs can be used and generated to increase protection, privacy and trust. We use one framework here, called Hyperledger [3], which is used to simulate the Blockchain network. Notice that Hyperledger, introduced in December 2015 by the Linux Foundation to support Blockchain-based distributed ledgers, is an open source Blockchain framework. Another one more example to simulate a decentralized platform is Enigma. This type of processing framework is completely decentralized and assures privacy and security, thus proving to be an evolution in the field of Blockchain. Enigma aims towards allowing developers to create 'privacy by design', end-to-end distributed software without the need for a loyal third-party. In general, Enigma-an extended allowance of Blockchain, is called so as its processing and data stocking cannot be achieved without Blockchain which acts as the operating system for it. Data is divided into different nodes which collaborate with each other and execute the functions without data leakage. Summing up, "there's never a single party who has complete access to data; instead, each party has a very random attachment of it." Fig. 3 details the algorithms and the approach used for the cryptographic techniques which have been adopted.

5.2. *Role of blockchain technology for building affordable, accurate, reliable and innovative (AARIN) approach*

Blockchain technology is used in our work as: a place to look where paper documentation is prevalent (i.e., key reasons for using the Blockchain network). Historically, paper documents were used in place of trust, i.e., you trust the paper certificate of authenticity instead of trusting the word of the merchant. The world has changed, however, and paper certificates are easy to duplicate or counterfeit, i.e. easier than digital signatures that are digitally signed. With assured validity and un-editable audit records, Blockchain will provide digital records. It is to be noted that each time a user wishes to upload his record/log, he is required to encode it fully. However, in our scheme, we have stuck to a similar but unique mechanism to encrypt the data. In spite of the fact that public key cryptography is extremely dependable on and trustworthy, the rate at which it encrypts data is way much slower than the original system. In fact, users create intricate access norms and regulations to control and handle data in a better way. This mechanism increases the ease with which the client can handle data, for example, it not only compels the people but the time for its access as well. Miner in Blockchain helps in distributing the data and details. Owing to the flexibility and constraints on tampering of data pertaining to Blockchain, miners can easily cross check whether each individual requester follows the control policies or not. Miners can also reduce the traffic levels and decrease the delay/propagation time on the network. Simultaneously, there exists a competent mechanism which can be picked. On the whole, the activity of the miners not just emphasizes and improvises the scheme, but trains to fight back intrusions from the adversaries. Via study, we illustrate that the system is not only safe and reliable, but can also provide protection of data to achieve privacy preservation. Our approach, therefore, is.

- Affordable: We used Light wright digital signature for small devices and light weight ring signature for along with digital signature to ensure anonymity of the user.

Algorithm 1: Data Encryption

1: **function** ENCRYPTION (data_ file)
2: **if** user confirm data preservation over blockchain **then**
3: Generate a symmetric key ksym
4: C ←Encrypts (data_ file, ksym)
5: Ck ← Encrypts (ksym, rkpub)
6: **else**
7: Do nothing
8: **end if**
9: end function

Algorithm 2: Ring Signature and Public key sharing

1: **function** SIGNATURE (data_ file)
2: **if** user chose anonymity over blockchain **then**
3: Generate an asymmetric public-private key pair sks pub, skspriv
4: hash p← calculate hash of the data_ file
5: Create the **Digital Signature** using hash p and signers private key skspriv
6: Share the public key skspub to the receiver using **Diffie–Hellman key exchange**
7: Mix the signature with another network group to form a ring
8: **end if**
9: end function

Algorithm 3: Data Decryption

1: **Input:** Encrypted file C, Encrypted symmetric key (Ck)
2: **Output:** Decrypted data_ file
3: **function** DECRYPTION (C, Ck, rkpriv, ksym)
4: ksym ←Decryptasym (Ck, rkpriv)
5: data_ file ←Decryptsym (C, ksym)
6: end function

Algorithm 4: Signature Verification

1: **Input:** Encrypted file C, Signers Public key (skspub)
2: **function** VERIFICATION (C, skspub)
3: hashc ← calculate hash of the received encrypted data file C to be verified
4: Using Public key skspub of signer, extract hashp of senders file
5: **if** hashc = hashp**then**
6: return C
7: **else**
8: return "Signature incorrect"
9: **end if**
10: end function

Fig. 3. Algorithms used.

- Accurate: Uses double encryption mechanism, one-time encryption mechanism for data and another one encryption mechanism for key to avoid any kind of alteration/attacks by hackers.
- Reliable: Data is received with ensuring integrity, i.e., not changed, destroyed, or removed.
- Innovative: We used the concept of MCPS based overlay network, i.e., dividing networks into several clusters (in place of proof of Work mechanism/single chain of Blocks) to reduce complexity.

Therefore, our approach to providing appropriate standards of protection and protecting user privacy in medical cyber physical systems is much better than other current models/frameworks. This chapter addresses the proposed work in depth. Now, the next section will address the outcome of the simulation with regard to our proposed work. Further, the readers can refer artile [18,36] for finding out several opprtunities towards Blockchain.

6. Simulation results/Security and privacy evaluation

Patients themselves are the owners of their medical data and are responsible for any other parties, such as insurance companies or healthcare providers, authorizing, refusing or revoking data access. They need to be very careful during accessing services through sensing devices/devices which have sensors in it. As discussed above, our proposed approach avoids attacks like man in middle, 51% attack, etc. Note that we find that few attacks like denial of service, mining, storages, dropping, etc., are still possible on our network. Also, challenges in IoTs devices are resource constraints of IoT, scalability, “high” investment cost, procuring IoT, interoperability, lack of government support/Immaturity of IoT standards, design-based challenge, security and personal privacy (data at rest, data in use, data in flight). Hence, this section discusses experimental results, i.e., performance of our proposed approach. In the next section, this work will conclude this work in brief (also will include future scope of our work).

7. Conclusions

One of the most important issues in academia and business today is privacy and protection in the IoT. Current safety solutions are not well suited because of the IoT resource constraint factor. Much of today's programs are used by CPS worldwide and have been celebrated for its promise that optimistic improvements and efficiencies in the provision of government services and a provocation for creativity and innovation in the private sector would be brought about. Yet, its privileges have been challenged and critiqued for extremes with respect to possible adversaries to privacy and security of individual content on account of the weaklings like biometric data, compulsory linkage with a number of applications and the chances of large-scale surveillance with the help of inter-related databases. With the continued debate, even today, the massive amount of data is produced with the help of IoT and which is more difficult to secure based on simple authentication schemes. When taking the IoT resource constraint element into consideration, our proposed architecture provides a solution to most security and privacy challenges. In this article, we proposed an innovative hybrid approach to create a patient-centered access control for electronic medical records that can offer security and privacy, incorporating the benefits of private key, public key, Blockchain and many other lightweight cryptographic primitives. We also pose a number of unanswered questions (in our work) to minimize numerous attacks such as DoS, but there are few major challenges to solving such problems when changing IoT resource constraints.

7.1. Future work

As discussed above, Blockchain, like every other technological application has drawbacks and limitations and cannot be implied to all scenarios with ease and flexibility. Blockchain techniques and its implications can revolutionize the future Internet systems and society. Today's Blockchain is also vulnerable and easily exposed a large number of challenges [25,37] and tasks from the technical aspects. Furthermore, certain consensus algorithms prefer proof of work or proof of stake in Blockchain are being exposed to serious issues. The issue of scalability needs to be addressed as it is a drastic issue [9]. Moreover, larger blocks imply increased storage space and reduced proliferation in the network [36]. Along with this, Blockchains are not perfect for high-frequency trading due to the delays brought about by the asynchronous, ad-hoc, peer-to-peer nature of the nodes participating in Blockchain (this can be resolved if, rather than storing complete transactional histories, the Blockchain hosts just an on-going verified representation of the transactions).

Today our biggest task is to protect user's data/CPS data with consuming less space and reducing accessing cost. But increased transparency in any technology does not necessarily mean the end of privacy. Security of CPS systems (stored sensitive information in a database) and stopping illegal breaching of this database is an essential and serious issue from a defense (a nation security) point of view. This (Blockchain) technology needs to clearly prove itself before conservative businesses take the plunge. In our research, we have put forth an effective and competent scheme which has its foundation on Blockchain for a network revolving around content and can assure users' data privacy. Furthermore, the sophistication of key controlling is highly reduced. In fact, we extract and make maximum use of the combined functionalities of access control policy and encryption techniques which promises data security and privacy. Only those clients who can supply the access strategy have the consent to acquire encoded data which is contained in the cloud. To protect our information/CPS system, we need to use/integrate some other technologies also to protect CPSs system/database/our personal network. So many questions raised here include “How a Blockchain is controlled”? Who controls it? Who gets access? Where are the servers? What physical and digital controls exist? Who monitors activity? And What will be the total for it? Once we receive answers to the above questions, then we will continue to improve the proof-of information algorithm in terms of efficiency and scalability. Using Blockchain, the all-medical records of concern are safeguarded and protected against any sort of unauthorized manipulations or changes. Making use of the Blockchain network is extremely compatible with respect to finance and efficiency as it eradicates the replication of efforts and decreases the urge for middlemen. Moreover, it's less exposed as it implements consensus models to verify details and thus, the transactions are safe, verified and authorized.

Note that the Blockchain is a technology that is still being developed, and the security research on it is still at an initial stage, and there has been little work done in this area. Finally, in order to prevent unnecessary energy consumption, the operating proofing mechanism is not appropriate. Instead of proof of work, we might propose Assigned Proof of Stake (DPOS) as potential work. The nodes involved in authentication and accounting purposes may be drastically reduced by DPOS. Through this, we will certainly reduce the management cost of network protection, optimize network efficiency, mitigate the cost of network control (bandwidth, CPU, etc.), etc. Thus, we will conclude that we need some creative ways to fix privacy issues using lightweight Blockchain, even though customers themselves execute public and private key transactions/processes. In short, our primary strategic direction for this work or any researchers wishing to undertake this work, apart from what has already been developed for all the individual cryptographic components used, is to incorporate the system into a testable system to provide some real guarantees of work security. We also aim to find an industry investor to help commercially make some of the creative ideas discussed in this study available. Finally, the realization of a self-powered Internet of Things is our ecological duty. One of the ways to prevent tons of battery waste and ensure stable and maintenance-free device functionality is the energy harvesting of wireless sensors. But to explore the exciting avenues

ahead, we need to do more research on this.

Author contributions

Dr. Amit Kumar Tyagi conceived this work, with original ideas, designed the schemes, and drafted this manuscript. Other authors have approved this manuscript for final publication.

Declaration of competing interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system [Online]. Available: https://bitcoin.org/bitcoin.pdf, 2008.
[2] http://crypto.marketswiki.com/index.php?title=Vitalik_Buterin.
[3] https://www.hyperledger.org/.
[4] Bikramaditya Singhal, Gautam Dhameja, Priyanshu Sekhar Panda, A Beginner's Guide to Building Blockchain Solutions, Book. Apress, 2018.
[5] Jesse Yli-Huumo1, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, Where Is Current Research on Blockchain Technology-A Systematic Review, PLOS ONE, 2016.
[6] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, Huaimin Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE 6thInternational Congress on Big Data, 2017.
[7] Pethuru Raj, C. Anupama, Raman, the Internet of Things Enabling Technologies, Platforms, and Use Cases, CRC Press, Taylor & Francis Group, 2017.
[8] Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal, Medical cyber physical systems and its issues, Procedia Comput. Sci. 165 (2019) 647–655. ISSN 1877-0509.
[9] A.K. Tyagi, G. Rekha, N. Sreenath, Beyond the hype: internet of things concepts, security and privacy concerns, in: S. Satapathy, K. Raju, K. Shyamala, D. Krishna, M. Favorskaya (Eds.), Advances in Decision Sciences, Image Processing, Security and Computer Vision. ICETE 2019. Learning and Analytics in Intelligent Systems, vol. 3, Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-24322-7_50.
[10] Amit Kumar Tyagi, T. Fredrick, Deepti Goyal, Shasvi Mishra, Blockchain Technology – A New Technology for Creating Distributed and Trusted Computing Environment, ICAAAIML-2020: International Conference on Advances and Applications of Artificial Intelligence and Machine Learning, 2020.
[11] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2019) 326.
[12] Tyagi, Amit Kumar and G, Rekha, Machine learning with big data (march 20, 2019). Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur - India, February 26-28, 2019.
[13] A.K. Tyagi, D. Goyal, A Survey of Privacy Leakage and Security Vulnerabilities in the Internet of Things, 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 386–394, https://doi.org/10.1109/ICCES48766.2020.9137886. Coimbatore, India.
[14] K.S. Reddy, K. Agarwal, A.K. Tyagi, Beyond things: a systematic study of internet of everything, in: A. Abraham, M. Panda, S. Pradhan, L. Garcia-Hernandez, K. Ma (Eds.), Innovations in Bio-Inspired Computing and Applications. IBICA 2019. Advances in Intelligent Systems and Computing, vol. 1180, Springer, Cham, 2021, https://doi.org/10.1007/978-3-030-49339-4_23.
[15] M. Shamila, K. Vinuthna, Amit Tyagi, A Review on Several Critical Issues and Challenges in IoT Based E-Healthcare System, 2019, pp. 1036–1043, https://doi.org/10.1109/ICCS45141.2019.9065831.
[16] Kumar Tyagi Amit, N. Sreenath, A comparative study on privacy preserving techniques for location based services, Br. J. Math. Comput. Sci. 10 (4) (July 2015) 1–25.
[17] A.K. Tyagi, S.U. Aswathy, Integrating Blockchain Technology and Artificial Intelligence: Synergies, Perspectives, Challenges and Research Directionsh, in: Advances in Blockchain Technology for Cyber-Physical Systems, Springer, 2021. Internet of Things Series.
[18] Amit Kumar Tyagi, Meghna Manoj Nair, Internet of everything (IoE) and internet of things (IoTs): threat analyses, possible opportunities for future, J. Inform. Assurance Secur. (2020).
[19] Latanya Sweeney, K-anonymity: a model for protecting privacy, Int. J. Uncertain. Fuzziness Knowledge-Based Syst. 10 (5) (2002) 557–570, https://doi.org/10.1142/S0218488502001648. October 2002.
[20] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, Muthuramakrishnan Venkitasubramaniam, L-diversity: privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data 1 (2007) 1, https://doi.org/10.1145/1217299.1217302. March 2007), 3–es.
[21] N. Li, T. Li, S. Venkatasubramanian, t-Closeness: privacy beyond k-Anonymity and l-Diversity, in: 2007 IEEE 23rd International Conference on Data Engineering, Istanbul, 2007, pp. 106–115, https://doi.org/10.1109/ICDE.2007.367856.
[22] Kumar Tyagi Amit, N. Sreenath, Preserving location privacy in location based services against sybil attacks, Int. J. Secur. Appl. 9 (12) (December 2015) 189–210 (ISSN: 1738-9976 (Print), ISSN: 2207-9629 (Online)).
[23] Cynthia Dwork, Aaron Roth, The algorithmic foundations of differential privacy, Found. Trends® Theor. Comput. Sci. 9 (3–4) (2014) 211–407, https://doi.org/10.1561/0400000042. August 2014.
[24] B. David, Meijer, Blockchain Technology, Trust and/or Control, 2017.
[25] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Generat. Comput. Syst. 88 (2018) 173–190. ISSN 0167-739X.
[26] L. Malina, J. Hajny, P. Dzurenda, S. Ricci, Lightweight ring signatures for decentralized privacy-preserving transactions, in: Proceedings of the 15th International Joint Conference on E-Business and Telecommunications, Porto, Portugal, 26–28 July 2018, pp. 526–531.
[27] M. Li, S. Yu, K. Ren, W. Lou, Securing personal health records in cloud computing: patient-centric andFine-grained data access control in multi-owner settings, in: S. Jajodia, J. Zhou (Eds.), Security and Privacy in Communication Networks, Springer Berlin Heidelberg, Berlin/Heidelberg, Germany, 2010, pp. 89–106.
[28] K.D. Mandl, D. Markwell, R. MacDonald, P. Szolovits, I.S. Kohane, Public standards and patients' control: how to keep electronic medical records accessible but private, BMJ 322 (2001) 283–287.
[29] Amit Kumar Tyagi, Cyber physical systems (CPSs) – opportunities and challenges for improving cyber security, Int. J. Comput. Appl. 137 (14) (March 2016) 19–27. Published by Foundation of Computer Science (FCS), NY, USA.
[30] N. Szabo, Smart contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, 1994. (Accessed 18 June 2018).
[31] G. Irving, J. Holden, How blockchain-timestamped protocols could improve the trustworthiness of medical science, F1000 Res. 5 (2016).
[32] A.K. Tyagi, A.M. Krishna, S. Malik, M.M. Nair, S. Niladhuri, Trust and reputation mechanisms in vehicular ad-hoc networks: a systematic review, Adv. Sci. Technol. Eng. Syst. J. 5 (1) (2020) 387–402.
[33] A. Josang, J. Haller, Dirichlet reputation systems, in: Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 10–13 April 2007, pp. 112–119.
[34] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017, pp. 618–623.
[35] Y. Chu, S. Rao, S. Seshan, H. Zhang, Enabling conferencing applications on the internet using an overlay muilticast architecture, SIGCOMM Comput. Commun. Rev. 31 (2001) 55–67.
[36] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Huaimin Wang, Blockchain Challenges and Opportunities: A Survey, Work Paper, 2016.
[37] Jin Ho Park, Jong Hyuk Park, Blockchain security in cloud computing: use cases, challenges, and solutions, MDPI (2017), https://doi.org/10.3390/sym9080164.