

Blockchain Based Secure Solution for Cloud Storage: A Model for Synchronizing Industry 4.0 and IIoT

Prakhar Sahu^{1,*}, S. K. Singh¹ and Arun Kumar Singh²

¹Amity Institute of Information Technology, Amity University Uttar Pradesh, Lucknow, 226028, India

²UBS, Commerzone, Pune, Maharashtra, 411006, India

*Corresponding Author: Prakhar Sahu. Email: prakhar.sahu@student.amity.edu

Received: 10 July 2021; Accepted: 15 July 2021

Abstract: Industry 4.0 is one of the hot topic of today's world where everything in the industry will be data driven and technological advancements will take place accordingly. In the fourth phase of industrial revolution, manufacturers are dependent upon data produced by the consumers to invent, innovate or change anything for the product. Internet of things devices like OBD, RFID, IIoT, Smart devices are the major source of data generation and represents trends in the industry. Since the IoT device are vulnerable to hackers due to its limitation, consumer data security should be tighten up and enhanced. This paper gives an overview of industrial revolutions as well as proposes Blockchain Cloud Computing as a solution to store data for Industry 4.0.

Keywords: Industry 4.0; IIoT; authentication; smart contract; ledger; P2P; IoT

1 Introduction

The term "Industry 4.0" was first quoted in Germany as a proposal for the development of a unique concept based on high-tech strategies for German Economic Policy. The concept marked the beginning of the fourth technological revolution based on concepts and technologies using cyber and physical systems, the Internet of Things (IoT) and the Internet of Services, which is based on continuous communication via the Internet and allows exchange of Information not only between humans and machines, but also between two or machines itself [1]. The term Industry I4.0 refers to the combination of several major innovations in digital technologies which includes advance robotics, artificial intelligence, sophisticated sensors, cloud computing, Internet of Things, big data analytics and many more. According to a third party data insight portal "Data Reportal", We are social and Hootsuite's report, more than 4.5 billion people were using internet by the starting of year 2020 which is the 60% of total world population. The report also suggests that more than half of world's population will start using social media by the middle of this year. In present scenario, 92% of the total world internet users are now connecting via mobile devices with 53.3% growth in comparison to 2018. The report says that an average internet user will spend 100 days online this year [2]. By 2025, around 37 billion connected devices are forecast, of which about 25 billion will be related to the IoT. Connected IoT devices include connected cars, machines, meters, sensors, point-of-sale terminals, consumer electronics and wearable's. At the end of 2019, there were around 1.3 billion IoT devices with cellular connections. This number is expected to touch 5 billion mark by the year 2025. The wide-area segment consists of devices using cellular connections, as well as unlicensed low-power technologies [3].



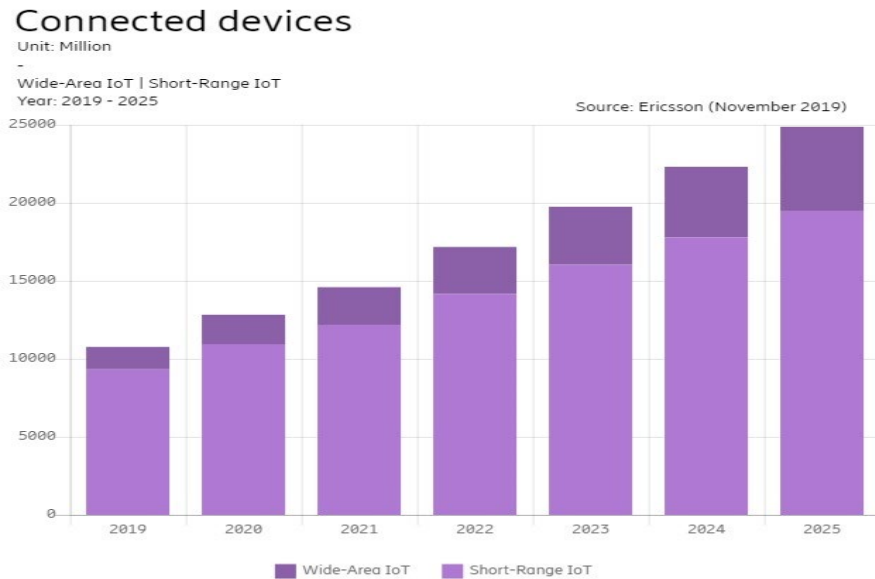


Figure 1: Connected devices

2 Industry 4.0 and Internet of Things

In the last 10 years, technologies have been evolved a lot and transformed from useful to a need of today's life. Internet of Things and Artificial Intelligence are one of them. When these two are combined, it opens the door of new possibilities. IoT and AI are transforming business models to make consumer oriented products and services. Businesses can now gather user data to convert it to a valuable insights with IoT [4]. Numerous reports speculates the number of IoT objects to reach 212 billion globally by the end of 2020 which has already passed the number of human existence over 2 times. In comparison to 2009, the data production will be 44 times greater with rapid increase in volume, velocity and variety of the data. This data (big data) cannot be processed through traditional algorithms and applications, it requires to be processed with the help of AI and Cloud computing to get better insights [5].

2.1 How Ready We are for Industry 4.0?

A research of Global Industrial Survey, 2017 shows that only 20% of the companies think that it does not affected them so far while 80% of the companies think that it has a significant impact on their businesses [6]. Industry 4.0 is different than last three revolutions, because it will challenge the existence of human where almost everything will be automated and precise. It requires big investments to implement from the companies. Apart from that, the government also needs better plans to regulate and ensure safety of the consumer data. I4.0 may also rise social tension by making job market a place divided into subcategories like low-skill/low-pay, high skill/high pay. The changes will be so fast that even those who are ahead of the knowledge curve may not be able to keep up with the changes [7].

2.2 India and IoT at a Glance

As per NASSCOM report on IoT, India will be among leading countries in IoT adoption in Asia Pacific region. India's IoT market is projected to be expand with the rate of 62% CAGR with \$9 Billion market by the end of 2020 consequently contributing to global IoT market revenue of \$1.1 trillion by 2025. To shape IoT industry in India, the Government of India has drafted some policies back in 2016. This draft draws an adaptive approach towards GoI's vision to build India a \$15 billion IoT market enabling India to hold nearly 5 to 6% of the Global IoT Industry [8]. India has also introduced Smart City Mission under which almost 100 cities are enrolled in. The smart city mission facilitates useful features like E-Mobility, Waste management, Water management, E-Governance, etc., impacting the total urban population of nearly 10 million.




2.3 Some Major Examples of Industry 4.0 Initiatives

Lamborghini, a supercar manufacturer shifted to I4.0 implementations with its new car Urus in the 80,000 sqm of surface built. This smart factory includes a Logistics center, Energy hub, Urus assembly line, Offices, Paintshop construction site, and finishing line under one roof. This smart factory consists of a few game-changing features like MES: Manufacturing execution system, Collaborative screwing system, Scan box: Automatic measuring machine, Virtual room to see the product & design before its finalization, Tyrebot: Automated tyre-fitting, AGV: Automated guided vehicles and Glass sealing collaborative robots. This smart factory also enabled its workers to control it remotely in their absence after I4.0 transformation impacting the reliance on paper documents and service quality [9]. The government of India created a platform called SAMARTH Udyog Bharat 4.0 to facilitate Industry 4.0 in various fields under the Ministry of Heavy Industries and Public Enterprises. This platform has various funded and non-funded ongoing projects with several case studies included. This platform is visioned to facilitate I4.0 standards to every Indian Manufacturing sector by 2025 with the help of ministries, industrial associations, and several R&D industrial institutions. A major car company Ford invested made \$690M investment as a part of EU600mn initiative in their Germany plant to automate the hot-forming process and replaced with robots and automated the process to ensure people’s and vehicle’s safety itself [10]. A Canadian printing solution provider Cober Solutions is robots designed & developed by OTTO Motors, an industrial automation company. These robots are used to transit raw material from one place to another. Prior to that, an operator had to stop their machines and take their finished goods to transfer them to another station. The whole process takes 10–15 min to do so. Now with the help of robots, the time is limited to 30 s, time is the key.

3 Security Challenges in Industry 4.0

Industry 4.0 is mainly based on cyber-physical systems and associated technologies. It brings useful improvements for data exchange and industrial control in the manufacturing industry. The interconnected nature of Industry 4.0 will add more risk to the user data and service inoperability. In the era of cyber warfare, Experts believe that traditional methods of defense may be not be useful. We need more cybersecurity strategies to be secured, vigilant and resilient as well as fully integrated into information strategy from the start. The list bellow elaborates the cyber risks related to their respective fields [11].

Figure 1. Smart production life cycle and cyber risk

Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Digital supply network 	Secure, vigilant, resilient	Data sharing	Ensure integrity of systems so private, proprietary data cannot be accessed
	Secure, vigilant, resilient	Vendor processing	Maintain trust when processes cannot be validated
Smart factory 	Vigilant	Health and safety	Ensure safety for both employees and the environment
	Vigilant, resilient	Production and process resilience/efficiency	Ensure continuous production and recovery of critical systems
	Vigilant, resilient	Instrumentation and proactive problem resolution	Protect the brand and reputation of the organization
	Secure, resilient	Systems operability, reliability, and integrity	Support the use of multiple vendors and software versions
	Vigilant, resilient	Efficiency and cost avoidance	Reduce operating costs and increase flexibility with remote site diagnostics and engineering
Connected object 	Secure	Regulatory and due diligence	Ensure process reliability
	Secure	Product design	Employ secure software development life cycle to produce a functional and secure device
	Vigilant	Data protection	Maintain the safety of sensitive data throughout the data life cycle
	Resilient	Remediation of attack effects	Minimize the effects of an incident while quickly restoring operations and security

Deloitte University Press | dupress.deloitte.com

Figure 2: Smart production life cycle and cyber risk

A report Attack Landscape H1 2019 by F-Secure shows that IoT was the top concern and favorite driver for internet attack traffic in the first half of 2019 [12]. A security firm Imperva reported a Mirai style attack using 400000 connected devices over the course of 13 days on online streaming application of an entertainment firm. This largest layer 7 DDoS attack botnet was producing more than 292000 request at a time [13]. iLnkP2P, a P2P solution (developed by Shenzhen Yunni Technology Company, Inc., China) that allows users to connect their devices to a computer or phone was found vulnerable to the hackers and yet being used in 2 million devices worldwide at the time of reporting. A security engineer Paul Marrapese, from the Bay Area, California first discovered a serious flaw also known as CVE-2019-11220 in January, 2019 that allows attackers to intercept connections to devices and perform man-in-the-middle attacks. Attackers may use this vulnerability to steal the password to a device and take control of it [14]. The developer showed his negligence and did not resolved this issue at their end causing serious trouble to the users and their privacy. These are the few examples of OEMs towards consumers' safety which should be seriously addressed.

4 Literature Review

According to the article written by Antonio Regalado, the rise of "cloud computing" term took place somewhere between 1996-97 by the small group of technology executives working in Compaq Computer [15]. In the year 2002, Amazon introduced their web-based retail services later other companies followed. In 2008, Eucalyptus offered first AWS API based cloud platform for private clouds. IBM (IBM SmartCloud, 2011), Apple (iCloud, 2011) and Oracle (Oracle Cloud, 2012) also introduced their cloud services. Further these services extended into IaaS (Infrastructure-as-a-service), PaaS (Platform-as-a-services) and SaaS (Software-as-a-service) [16]. The fourth industrial revolution is based upon cyber physical systems turning conventional factories into smart factories where everything is data driven and automated at large scale. The way we are moving toward data revolution, it is necessary to adapt decentralized cloud computing technologies. In a centralized data centre, your data stays inside giant data centres if the server goes down, your access to the data is lost. In decentralized cloud computing, data is saved on multiple locations so the access is not interrupted when one server is down. From a security point of view, decentralized cloud computing is complex and secure in comparison to conventional cloud [17]. Chandra et al. discussed about a volunteered decentralized cloud solution called Nebula. The author also described the properties and design issues [18]. Shah et al. proposed a system for decentralized secure data storage IPFS (InterPlanetary File System) in a blockchain system using MetaMask and Web3.js. For reliability and availability, the data is replicated in at least 3 peers [19]. Scoca et al. proposed a calculation model suitable to analyse and verify the properties of smart contracts using dSLAC language. The author developed a compatibility with some use cases [20]. Mohanta et al. explained the working principal of Smart Contracts along with the blockchain integration and use cases in different scenario. The author also outlined the challenges may arise during and after the implementation of smart contracts in real world [21]. Zheng et al. explained the overview of Blockchain and Smart Contract by giving a simple example of transaction between a buyer and a supplier. The author also has also compared some existing models and their compatibility on several platforms [22]. Song et al. designed a decentralized end user computing service platform to distribute edge computing to users. The technology works on smart contract based encryption and distribution system for access control [23]. Feng et al. suggested a model using decomposition method and divided smart contracts into sub contracts for execution. The author also discussed about various aspects of the model suggested [24].

5 Smart Contract as a Secure Solution for Cloud Storage

Smart Contracts are the vital part of Blockchain technology introduced in 1990s as a computer transaction protocol to execute the terms of contract. Although it can also be implemented on other platforms too. Smart contracts refer as a set of rules specified in digital values which also includes protocols, parameters and limitations. In a Blockchain network, every smart contract has a unique address

to trigger a transaction. It executes in a predefined manner on every node of the network according to the data included while triggering the transaction.

Table 1: Use cases of smart contracts

Digital Identity	Smart contracts can help individuals to own and control their digital identity, it will help them to choose what to share with counterparties [25].
Financial Data Keeping	For transparent recoding of financial data and accurate analysis, Smart contracts may be used. It improves financial reporting and reduce auditing and assurance costs [25].
Supply Chain	Smart contracts provide transparency at every level of a supply chain like how a product moves from factor to a consumer’s shelf with real time updates [25].
Copyrights	Organizations like music industry, film production house, etc., can use smart contracts as a copyright agreement that would help keeping track of ownership rights and royalty distribution. It will ensure true ownership among the contributors [26].
Internet of Things	Internet of Things devices are becoming integral part of cyber physical systems, considering the present scenario use of smart contracts in IoT device will help improving IoT more autonomous [27].

In the fog layer, a local server is installed at the premises used for analysis and storage purposes. The central server is usually located on cloud somewhere far from the branch and used only for data storage using blockchain cloud storage technology.

6 Suggested Model

Foreseeing the events of major attacks on several companies, it is very important to focus on the security of cyber-physical systems in an organization. To overcome this challenge, a suggestive model is presented using smart contracts for cloud computing implementation for Industry 4.0. The suggested model completes in 4 parts. 1. End Devices, 2. Data Collection, 3. Data Classification, 4. Data Storage. Fig. 3 previews a layout of a usual unit in a car factory in terms of Industry 4.0 and Smart factory implementations.

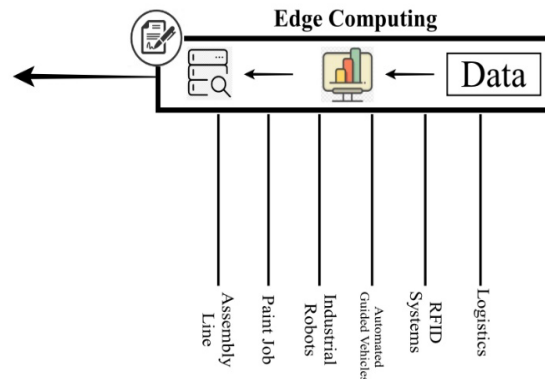


Figure 3: Overview of a single unit or a department

Table 2: Abbreviations used

End Devices/User	Usually the IoT devices like RFID, Conveyor Belt, Access control, etc., that are interconnected either manual or automated.
Data Collection	At this step Data is collected from various data sources like Devices, Departments, Equipment.
Data Classification and Analysis	At this step data is sent to the processing unit installed at the fog layer for analysis. After analysis, processed data is segmented into two parts, Important and Not-Important. The important data stays in the cloud and the rest are ignored.
Storage	At this step Once the data is analysed, it is stored to the cloud server for access and available to all.

Smart Contracts	Set of instructions and terms used for each transaction, automatically executes.
Edge Computing/Fog Layer	The end point of all the connected devices from where the data is fetched and sent for analysis/storage.

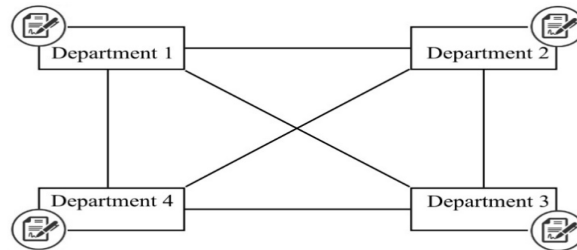


Figure 4: Overview of a suggested model

Fig. 4 shows the interoperability between various departments/locations at different points. All of the are internet connected via high speed internet. Each department has their own fog layer (Edge Computing) and smart contracts installed. An end user/device in department 1 sends a command to execute an action. The device completes the action, it generates some data, the data gets processed further stored in a local cloud server. Flowchart in Fig. 5 elaborates the working mechanism of authentication process using Smart Contract in smart factory environment. In this process, authentication is started with a request of “Source A”, The server will ask for smart contract from Source A. If the SC is fetched, it will be redirected to the other connected servers for authentication (e.g., Server X where last character “X” represents the initial of a connected server followed by Y, and so on). The server will verify the SC with the list called ledger present in their own server which gets updated after every incoming/outgoing transaction. Once the verification is done the counter will increase by 1 and the request will be moved to another server and the process will be repeated till the request is verified from all the sources (see Fig. 5).

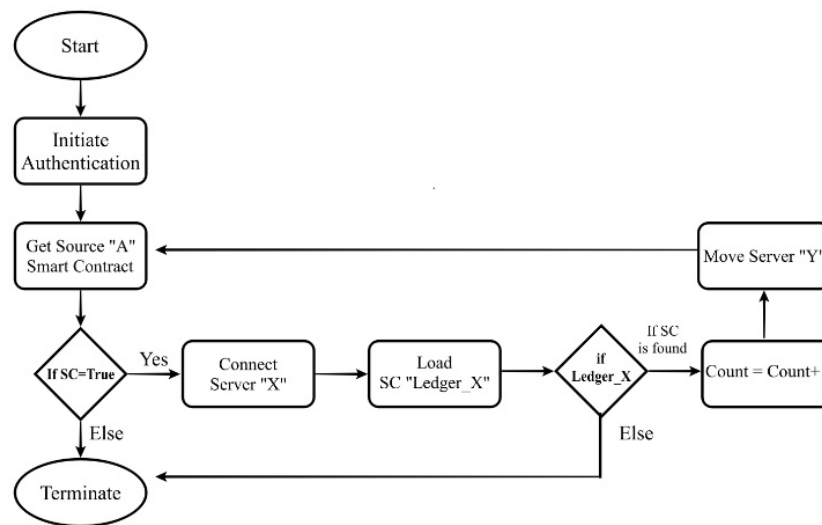


Figure 5: Flowchart of smart contract authentication system

Once all the sources completes the verification the process will be terminated and the counter value will be checked using this formula.

6.1 Percentage Calculation Formula

```

Percentage = Count * 100 / Total Number of
Servers
If Percentage >= 75
{
Access granted
else
terminated
}

```

Example: Suppose that a Technician sends command to an automated robot to transfer a parcel No. 1 to transfer to a conveyor belt from location A. The robot will go through a predefined path, reach to the parcel where it is located. It will scan the barcode of the parcel using barcode scanner and once and once it is verified it will be transferred and placed on location A. At this stage so many data is gathered like path, source/destination's location, barcode, robot ID, user's name, etc., but it has only few data is important like Barcode, Robot ID and the location itself. Important data in this case is stored to the server and the rest is ignored.

Table 3: Verification and validation

Properties	Model 1 [28]	Model 2 [29]	Model 3 [30]	Proposed model
Authentication framework	Blockchain, P2P	SC, Blockchain	SC, D2D, D2G	SC, Ledger
Applications	Cloud	Wireless networks	Cloud, IoT	Cloud, IoT, Localhost
Impact area	Data integrity	Wireless networks	Smart farming	IIoT, IoT

The proposed model has many advantages to implement like In the current scenarion, so many data are gathered like path, source/destination's location, barcode, robot ID, user's name, etc. Out of these gathered data, only few data is important like Barcode, Robot ID and the location itself. Using this model, important data is stored to the server and the rest is ignored. This will improve the system performance. The data is gathered from the connected devices/machines and stored on a local server which is further shared to the cloud with some limitations and filtering. Since the data analysis is done at the local level, there is no need to create a centralized server that saves storage and makes the model cost effective. If an intruder somehow manages to get access to a local unit/department, the threat will be limited to that department only and may be resolved easily.

The main objective of this model is to create a secure environment for smart factories under the Industry 4.0 standards. This model will also help reducing processing time and unusual traffic on the network since most of the processing is done in the fog layer and data is locally stored in independent units.

7 Conclusion

Industry 4.0, IIoT, Cyber Physical System, Blockchain Cloud Computing, I4.0 integrity of the data play an important role in smart factories where everything is data dependent. Use of blockchain in the industry will build trust but should be standardized as per the required properties for Industry 4.0 standards. The proposed Blockchain as a secure solution for cloud storage based model which works on a P2P mechanism will be of great help because it ensures the sharing of distributed ledger with every participant with updation taking place after every transaction in the network.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] V. Roblek, M. Meško and A. Krapež, “A complex view of Industry 4.0,” *SAGE Open*, vol. 6, no. 2, 2016.
- [2] S. Kemp, “Digital 2020: Global digital overview,” Datareportal.com, 2020.
- [3] “Ericsson mobility visualizer,” 2020. [Online]. Available: <https://www.ericsson.com/en/mobility-report/mobility-visualizer?f=13&ft=3&r=1&t=18&s=9,10&u=1&y=2019,2025&c=1>.
- [4] R. Schmelzer, “Making the Internet of Things (IoT) more intelligent with AI,” 2019. [Online]. Available: <https://www.forbes.com/sites/cognitiveworld/2019/10/01/making-the-internet-of-things-iot-more-intelligent-with-ai/#1ac1df41fd9b>.
- [5] “Artificial intelligence for cloud-based Internet of Things (IoT),” 2018. [Online]. Available: <https://www.journals.elsevier.com/future-generation-computer-systems/call-for-papers/artificial-intelligence-for-cloud-based-internet-of-things-i>.
- [6] B. Ślusarczyk, “Industry 4.0—Are we ready?” *Polish Journal of Management Studies*, pp. 232–248, 2018.
- [7] B. Marr, “forbes.com,” 2018. [Online]. Available: <https://www.forbes.com/sites/bernardmarr/2018/08/13/the-4th-industrial-revolution-is-here-are-you-ready/#31190027628b>.
- [8] R. Rahul and S. Rajeev, “Future of IoT,” 2019. [Online]. Available: <http://ficci.in/spdocument/23092/Future-of-IoT.pdf>.
- [9] S. Souchet, “Industry 4.0 case studies: The KPMG case for i4.0 success,” [Online]. Available: <https://home.kpmg/xx/en/home/insights/2018/11/industry-4-0-case-studies.html>.
- [10] S. Galea-Pace, “Putting safety first through digital transformation at Ford,” [Online]. Available: <https://www.manufacturingglobal.com/lean-manufacturing/putting-safety-first-through-digital-transformation-ford>.
- [11] W. René, L. Tyler, H. Ramsey and C. Robert, “Industry 4.0 and cybersecurity-Managing risk in an age of connected production,” 2017. [Online]. Available: <https://www2.deloitte.com/us/en/insights/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html>.
- [12] M. Michael, “Attack landscape H1 2019: IoT, SMB traffic abound,” 2019. [Online]. Available: <https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/>.
- [13] V. Simonovich, “Imperva blocks our largest DDoS L7/Brute force attack ever (Peaking at 292,000 RPS),” 2019. [Online]. Available: <https://www.imperva.com/blog/imperva-blocks-our-largest-ddos-l7-brute-force-attack-ever-peaking-at-292000-rps/>.
- [14] P. Marrapese, “Security cameras vulnerable to hijacking,” 2019. [Online]. Available: <https://hacked.camera/>.
- [15] A. Regalado, “Who coined ‘cloud computing’?” *MIT Technology Review*, 2011. [Online]. Available: <https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/#:~:text=The%20notion%20of%20network%2Dbased,term%20to%20an%20industry%20conference.&text=We%20call%20it%20cloud%20computing,a%20%E2%80%9Ccloud%E2%80%9D%20somewhere.%E2%80%9D>.
- [16] K. D. Foote, “A brief history of cloud computing,” *Dataversity*, 2017. [Online]. Available: <https://www.dataversity.net/brief-history-cloud-computing/#>.
- [17] Medium, “What is decentralized cloud storage,” Storj Labs, 2020. [Online]. Available: <https://medium.com/@storjproject/what-is-decentralized-cloud-storage-3a530f1552>.
- [18] A. Chandra, J. Weissman and B. Heintz, “View from the cloud: decentralized edge clouds,” in *IEEE Internet Computing*, Abhishek Chandra, Jon Weissman, 2013, pp. 70–73.
- [19] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, “Decentralized cloud storage using blockchain,” in *Proc. of the Fourth Int. Conf. on Trends in Electronics and Informatics*, 2020.
- [20] V. Scoca, R. B. Uriarte and R. de Nicola, “Smart contract negotiation in cloud computing,” in *IEEE 10th Int. Conf. on Cloud Computing*, Honolulu, CA, USA, 2017.
- [21] B. K. Mohanta, S. S. Panda and D. Jena, “An overview of smart contract and use cases in blockchain technology,” in *9th ICCCNT*, Bengaluru, 2018.
- [22] Z. Zheng, S. Xie, H. N. Dai, W. Chen, X. Chen *et al*, “An overview on smart contracts: challenges, advances and platforms,” *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.
- [23] J. Song, T. Gu, Y. J. Ge and P. Mohapatra, “Smart contract-based computing resources trading in edge computing,” in *IEEE 31st Annual Int. Sym. on Personal, Indoor and Mobile Radio Communications*, London, UK, 2020.

- [24] T. Feng, X. Yu, Y. Chai and Y. Liu, “Smart contract model for complex reality transaction,” *International Journal of Crowd Science*, vol. 3, no. 2, pp. 184–197, 2019.
- [25] Smart Contracts Alliance, “Smart contracts: 12 use cases for business & beyond,” 2016. [Online]. Available: <http://digitalchamber.org/assets/smart-contracts-12-use-cases-for-business-and-beyond.pdf>.
- [26] Skalex, “Smart contract application examples and use cases,” [Online]. Available: <https://www.skalex.io/support/blockchain/smart-contracts/use-cases/#contact>.
- [27] K. B. Mohanta, S. S. Panda and D. Jena, “An overview of smart contract and use cases in blockchain technology,” IEEE, 2018.
- [28] D. Yue, R. Li, Y. Zhang, W. Tian and C. Peng, “Blockchain based data integrity verification in P2P cloud storage,” in *2018 IEEE 24th Int. Conf. on Parallel and Distributed Systems*, Singapore, 2018.
- [29] G. Li, Y. Wang, B. Zhang and S. Lu, “Smart contract-based cross-domain authentication and key agreement system for heterogeneous wireless networks,” *Mobile Information Systems*, vol. 2020, 2020.
- [30] A. Vangala, A. K. Sutrala, A. K. Das and M. Jo, “Smart contract-based blockchain-envisioned authentication scheme for smart farming,” *IEEE Internet of Things Journal*, 2021.