The Blockchain-Based Decentralized Approaches for Cloud Computing to Offer Enhanced Quality of Service in terms of Privacy Preservation and Security: A Review.

Arun Kumar B.R.[1], Komala R[2]
[1]arunkumarbr@bmsit.in [2]komal.uday@gmail.com

[1] Professor, Department of Computer Science and Engineering and Research Supervisor, VTU Research Centre, Department of MCA, BMS Institute of Technology and Management, Bangalore, India

[2] Research Scholar, VTU Research Centre and Asst. Professor, Department of Computer Applications, REVA University, Bangalore, India

Summary
In the recent past enormous enterprise applications have migrated into the cloud computing (CC). The researchers have contributed to this ever growing technology and as a result several innovations strengthened to offer the quality of service (QoS) as per the demand of the customer. It was treated that management of resources as the major challenge to offer the QoS while focusing on the trade-offs among the performance, availability, reliability and the cost. Apart from these regular key focuses to meet the QoS other key issues in CC are data integrity, privacy, transparency, security and legal aspects (DIPTSL). This paper aims to carry out the literature survey by reflecting on the prior art of the work with regard to QoS in CC and possible implementation of block chain to implement decentralised CC solutions governing DIPTSL as an integral part of QoS.

Keywords:
Block-chain technology, cloud computing, decentralized, privacy, security, transparency, trust model, quality of service.

.1. Introduction

Cloud computing (CC) has grown and successful in offering technical as well as economic benefits [1]. Enterprises including start-ups by adopting CC can get the rid-off risk of capital investment by cutting cost towards hardware and software infrastructure and avail of the services as per their demand. The CC technology has beautified the hardware and software by enabling its operators to provide rich offers including "Infrastructure-as-a-Service (IaaS)", "Platform-as-a-Service (PaaS)", and "Software-as-a-Service (SaaS)" solutions along with public, private, and hybrid architectures adoptions [2]. These basic service paradigms are predominant and indicate the services that CC accomplishes.

Most simply, IaaS can be thought of as providing access to infrastructure such as additional data backups for business data storage, offering required bandwidth for a commercial website server. The IaaS services such as Amazon EC2, Google's Compute Engine (GCE), and IBM Soft Layer are powered the of the internet services. PaaS model as defined by Gartner offers a platform on which end users are allowed develop their own application, execute, and accomplish applications. PaaS conceptually acts as a middleware between SaaS and IaaS. Platforms such as Google's App Engine, IBM BlueMix, and Apache's Stratos are prevalent PaaS products that are facilitating to rationalize and democratize software development.SaaS is a model of service called 'on-demand software', where it affords software which is a fully functional product along with licensing to subscribed end users typically over the web. Widespread products namely Salesforce and Office365 have put SaaS to the front position of the place of work of thousands of businesses every day.

The CC industry has an average growth rate of 46.33 % since 2016 [10]. Gartner, predicts that CC business will reach $300 billion by 2021 [11] as successful players such as Apple, BMC are in the industry followed by well-established start-ups such as BoX and Workday, etc. bringing innovative features in the market. The technological innovations and, thousands of new features lead to complexity at a higher level and muddles customers especially about security and privacy of data. No doubt, CC has greatly simplified and magnificently marching towards offering QoS by automating hardware and software resource allocation as per the demand of the applications to meet expected performance, reliability, and availability along with trade-off between operational cost and quality [3][4]. The applications offered by Cloud Service Provider (CSP) are generally shared by multiple users and further programming interfaces provided enables customers to build, deploy applications on the cloud and store enormous data. However there is no idea for the customers regarding the location, data storage, the privacy offered to data, and the type of hardware infrastructure used [6]. Therefore we can say there exists a poor trust model. The service level agreement is the only means to represent the QoS

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.16

requirement to the customer. By implementing the smart contracts in the blockchain network CC can enable dynamic service agreements and ensure implementation of the trust model. This implies that CSP can assure enough QoS guarantees to the customer without middlemen or human element interference.

Majority of the research work with respect to CC Quality of service (QoS) is the deal of measure of the performance in the perspective of users. However, security and privacy in CC is rarely focused. It is high time to realize the other dimension of the users perspective to protect data privacy and continue to meet user expectation. Further, exuberant growth of cloud computing services motivates to relook into significant technical issues related to privacy preserving protocols, mechanisms for security threats and decentralised CC. Even though QoS issues have drawn the attention of quite a good number of researchers constantly and investigations have contributed in the right direction, cyber-attacks and privacy concerns have created a need to investigate the security aspects in protecting the data integrity, reliability, and privacy by adopting the block-chain technology (BCT). These aspects of security will greatly enhance the QoS and prompt several interested researchers to QoS analysis, design, and implementation using BCT.

This paper aims at summarizing the prior art search concerning the implementation of block-chain-based decentralized (BBD) CC which can bring several transformations to guarantee the QoS to the customer/enterprise. The paper briefs on regular basic parameters of QoS and focuses on DIPTSL to establish the trust to store the confidential data and still use CC as a platform to execute their businesses.

1.1 Scope.

The CC has a large area of coverage including business applications, e-governance, automotive systems, multimedia services, process control, and finance [5]. The rich literature survey describes comprehensively QoS models of CC but is confined to largely on the modelling of workload, system, and their applications to QoS management such as [3]. This paper focuses on literature survey of BBD applications along with smart contracts in the literature survey to CC problems. Further, the computing limitations of IoT devices need additional security layer to validate the data and store securely in the cloud.

1.2 Methodology.

The research work explores the early work of blockchain applications and its scope in CC QoS models, introducing readers to specific technical and economic benefits. Specifically, the paper focuses on the works published from 2012 on DIPTCL privacy issues in CC. Furthermore, the survey analyses the security of data generated by IoT devices in different sectors and its storage in Clouds.

2. Organization of the survey analysis

This paper covers research efforts for QoS models in CC and blockchain applications to CC with a decentralized approach. The paper has organized the summary of the survey into the following subcomponents:

(i) General CC QoS models
(ii) BBD implementation in CC
(iii) BC in CC for DIPTSL QoS parameters

2.1 CC QoS models

In the literature models such as Workload, System, and application are adopted to ingrain the QoS. Workload modeling involves the assessment and predictions of request and allocation of resources such as CPU, memory as per the application requirements. The model needs to dynamically allocate and deallocate the various resources and analyze whether the assured QoS level is met. System modeling evaluates the CC performance in terms of response and run time to meet the cloud application performance. Application QoS model is related to optimized decision making in managing the system for resource allocation, balancing the load and admission control from the CSP and end-user perspectives at the same time minimizing the operational cost [3]. Workload characterization needs to analyze the deployment environment including web traffic intensity at different time scales to know congestions/bottlenecks, the pattern of bandwidth variations, prediction of available bandwidth and ensuring application bandwidth requirements, virtual machine performance, and other network overheads.

It is significant to characterize the workload handled by cloud application for resource allocation as refereed in [7]-[9]. The latest work such as [7] is pertaining to workload characterization uses Hidden Markov Models (HMM) to create cloud clusters with resource predictions to the provision of the resources and analyze the server workload pattern. The work in [8] explains “long-term workload prediction and pattern analysis”, validating results by applying the Bayesian algorithm on large scale data from a

Google centre. The application of pattern recognition methods to data centers and cloud workload data to efficiently allocate servers to different workloads is discussed in [9]. As reported in one of the surveys, CC is at the peak of the risk list[12] which is predominantly related to security and privacy, advent of new features have attracted attackers as a new target which may affect operations of CC leading to massive downtime in their network [12]. The next section, discusses security, privacy, and legal aspects as a part of QoS.

2.2 Need for Blockchain based decentralised approach

As pointed out by Bruce Schneier, a well-known cryptographer, CC may miserably fail to meet legal requirements of a company [13]. Mr. Schneier states that cloud providers may fail to meet a company's legal needs. The CC technology stores data quite often in multiple data locations which may include outside the "European Economic Area "(EEA). As implied by the recent " EU General Data Protection Regulation" (GDPR), CC projects have obligations to adopt infrastructure changes to be regulatory compliant. Losavio et al., in their work [30] [R1] highlighted that the trustworthiness of data is a key concern of all stakeholders and applications need to follow governmental regulation. In this direction CC must comply with existing as well as anticipated standards in the ever changing infrastructure dynamics. Further, the inherent cross jurisdiction nature of CC has added additional complications in data protection, privacy, IPR and self as well as government regulation.

Further it is necessary to assure the QoS as per the privacy requirements of the company and implement data control measures as expected by the customers. Security, privacy and legal issues are at high risk since CC systems are centralized. Further, the design issues of CC which reduces the network down time and cyber-attacks which are considerably pushed CC to high risks are to be addressed immediately [14]. Enormous amount of data gets generated at the global level, IDC predicts that IoT market capital, efficiency, economic benefits will improve greatly by 2021[15]. it should be noted that IoT also leads to generation of high amount of data [16][17][18[19][20][21]. As estimated in [19], people, machines, and things engender more than 850 Zettabytes by the end of 2021. The idea of centralised CC is no longer continue to be valid as demand for CC service is exponentially increasing that in turn increases the volume and velocity of data and business processes are expected to completed at a significantly faster pace than ever before. This is significant point to be noted as per Gartner and motivates to move towards decentralised approach. [23], [24], [25].

Further, it is challenging in CC with centralised infrastructure to able to support such a huge data by guaranteeing security, scalability, privacy, legal requirements of the company and still optimizing the resources with concurrency?". Blockchain is an immutable, middlemen free, cost effective, enables legal as well as regulatory aspects, terms and conditions of the business supply chain through smart contracts, distributed, ledger of transactions which can be programmed. It is disruptive technology which is not limited to financial transactions, cloud computing, smart-IP, trademark infringement or patent infringement, digital asset management, legal compliance through smart contracts [26].

The worldwide interest in the blockchain has prompted researchers to think of this technology with CC. The massive accidental data leakage of 198 million Americans as noted in the case of "" Deep Root Analytics has proved the vulnerability of the centralized approach of the CC. This will lead to blockchain based CC with hybrid approach [26] in the futures to come. Even though the blockchain technology is a very complex process suitable modifications can boost and enables continues improvement of CC marketing.

2.2.1 Blockchain-as a decentralised approaches and key challenges

Wherever CC technology offers resource sharing services scalability is a bigger issue since dependency is on central nodes, hence it is a good idea to introduce nodes which can provide computational power and validate the transactions in a distributed manner, avoid misbehaving nodes, and at the same time, such nodes who provides computing resources online can be encouraged by providing incentives. This is possible due to the implementation of blockchain technology which can support decentralized, privacy protected, transparent, legal CC solutions.

Even though blockchain-based CC solutions appear to be attractive, there are several challenges as defined by Prof. Brundo Riarte and Prof. De Nicola [23]. Some of the challenges described are:

- ✓ Implementing a correct enticements strategy to offer fair revenue distribution for resource suppliers.

- ✓ Overcoming the present scalability issues of blockchain infrastructure.
- ✓ Defining the right strategy for verifying the manner of computation execution.
- ✓ Implementing the trust model through smart contracts that alleviate the trust issue [28, 29].
- ✓ Security mechanisms to implement eraser in case of a malicious attack or any other unexpected event happens.

There are enormous projects going on proposing novel ideas to implement blockchain to offer decentralized computing solutions. Some use cases of blockchain due to the Ankr, Dfinity, and Solana projects that are presented in the next section.

2.2.2 Blockchain-based decentralised CC solutions

(a) Ankr

The decentralized CC solution aimed to bid customers the infrastructure services at competitive prices lesser than traditional cloud services is the goal of the Ankr project [27]. The project plans to offer enhanced service availability, secure communication utilizing containerization, cluster orchestration (CO), and a Trusted environment for execution (TEE). The drawbacks of virtual machines such as consumptions of huge resources (CPU & RAM), taking minutes to start, complex development resources are eliminated by leveraging containerization and underlying CO. TEE provides memory area for execution which is protected even on compromised platforms. The novel consensus contrivance developed in [27] has the ability to offer high security with minimal energy called Proof of Useful Work (PoUW) as explained in [10]. Figure 1 shows the crucial component of Ankr's mining pattern.

(b) Dfinity

This project talks about implementing supercomputer with infinite capacity with the concept of " The AI is Law" which is contradictory to bitcoin and ether where "the code is the law". In the Dfinity project with the approval of the programmed governance system, the transactions can be reverted back. The consensus contrivance assembly is shown in Figure 2 below. As explained in [28][29] and [10] consensus tool enables the infrastructure to scale consistently , with a fair scheme and security.

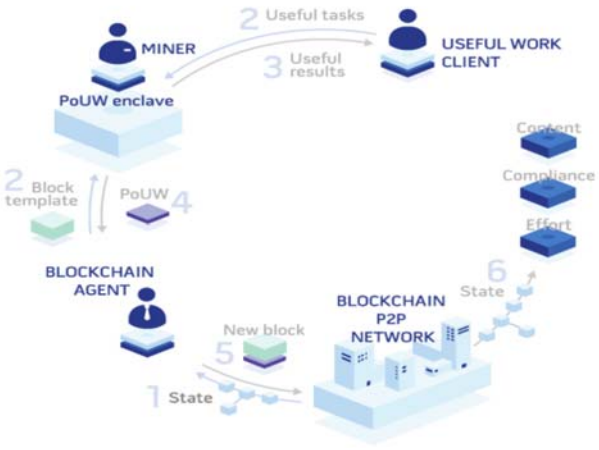

Figure 1: Ankr's Proof of Useful Work consensus overview (source : Ankr [27] (2018)

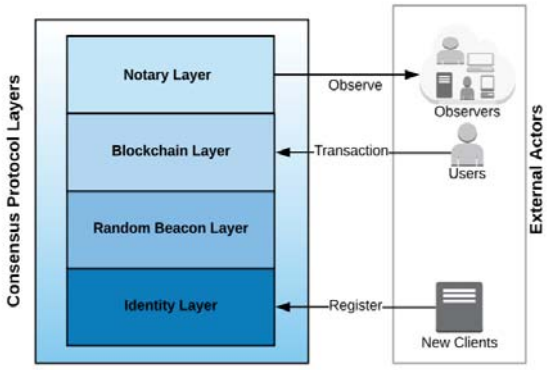

Figure 1: Figure 2: Dfinity's consensus mechanism layers (Source : Dfinity [28] (2018))

(c) Solana

The intention of the Solana project [30] is to organize the blockchain architecture on the concept of Proof of History (PoH). The GPUs handle the transactions based on Moore's law which allows much more computational power. This mechanism when combined with the Proof of Stake (PoS) consensus algorithm makes the infrastructure highly scalable with decentralization as explained in [30] and [10]. Additionally, transaction processing on Solana is handled by GPUs, an approach that uses Moore's law to allow additional computational power. This mechanism, used in combination with a Proof of Stake (PoS) consensus algorithm, can make the infrastructure highly scalable. The transaction flow that happens in Solana is shown in Figure 3.

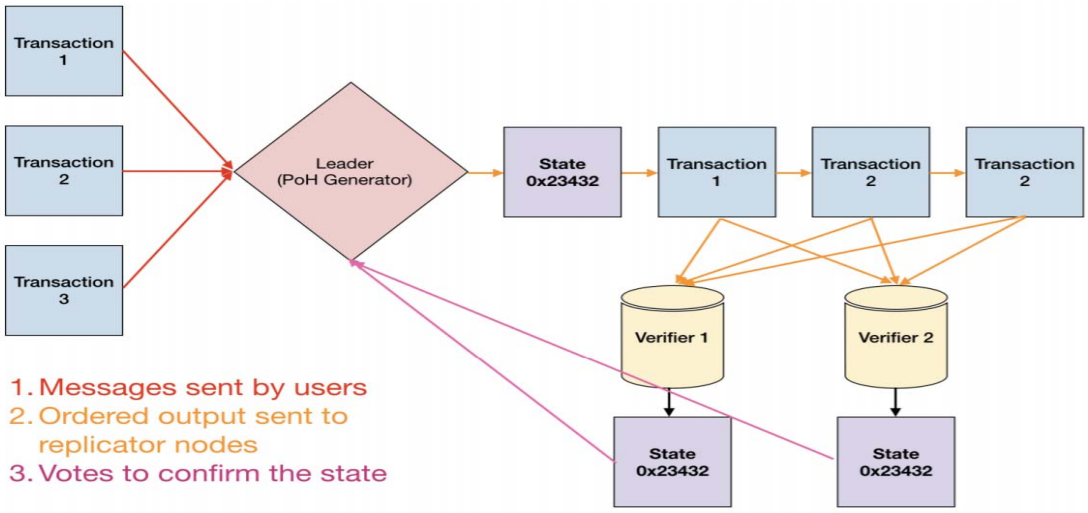

Figure 3: Transaction flow in Solana network (Source: Solana [29] (2018))

2.3 BC in CC for DIPTSL QoS parameters

2.3.1 Data integrity (DI)

DI is an invaluable asset, influences decision making in all business. Thus DI makes its relevance , especially in CC , the issue is more exacerbated since the physical location of data is not known and data owner hardly control its access [31] ,[32]. Since very large number of organization think of reducing the cost of data storage and maintenance locally [33] , the demand for CC services is ever increasing. As per the Gartner report [34], global market has grew 37.3% in 2019 on cloud IaaS platform. There will be a continuous demand for cloud services due to Coronavirus pandemic [34] .This implies that DI is a critical issues to be addressed on highest priority [35]. The work in [33] investigates and proposes effective BBD that allows trade-off among integrity guarantee, performance and stability. The idea is to implement lightweight consensus mechanisms and pulls on the supremacy of PoW only in the background. The investigation in [37] explores BCT in CC domain and analyses the "issue of block withholding attack ". The method discussed in [R8] for DI uses the "distributed ledger using consensus algorithm " to keep track of an untampered state of deposited data.

2.3.2 Privacy

Data can be broadly classified as public and private, further private data can be classified as personally identifiable information (PII) and sensitive data[39]. Private data can be belonging to a person or organization. Violation of privacy is using the private data without the consent of the concerned person/ organization. Every nation has its own the legislation governing the data privacy. Largely many countries have derived U.S.A. legislation called "The Fair Information Practices (FIP)" [40]. The report in [41] governs the " protection of individuals with regard to the processing of personal data and on the free movement of such data". To maintain data privacy industry and organization have to adopt legal standards as per the law of the nation such as The Safe Harbor agreement [42] and international standard for CC [43]. In India, data privacy is governed by the "Information Technology Act, 2000 (**IT Act**) " and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**") [44].The CSP along with legal obligations are required to adopt technology to meet the assured privacy to the user. The work in [45] adopted blockchain-based "access control framework with privacy protection" called AuthPrivacyChain.

Smart contract is expected to play significant roles for privacy protection, the work in [46] highlights on " Block chain based smart contract using AI is proposed for privacy protection " . In [47] the different methods for implementing smart contract for privacy protection is discussed. Further, for preserving privacy in the cloud computing " Secure Multi-party Computation and Zero-knowledge Proofs " were investigated.

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.16

3. Conclusions

This paper gives an overview of the traditional QoS models of CC and the growing demand for CC in the industry market. The lacunae in the current CC technology, need for a decentralized approach in the perspective of the exponential growth of IoT devices and their data generation and legal requirements of the company. The crucial use cases where blockchain-based decentralized CC solutions have been presented which explain implementing consensus mechanisms among the parties.further, it is highlighted regarding DI and privacy of data in CC. Blockchain-based decentralized CC solutions are still in their early period and, for this reason, scalability, and performance and as a part of QoS, security, privacy, and legal aspects are important to foster the economic growth in CC marketing. Blockchain-based solutions with suitable modifications can enable us to achieve the additional parameters of the QoS.

The new and ingenious technology, blockchain allows participants to validate the blocks of data and store same copy of data across immutable registers .Thus data becomes open and secure in the agreed network of stakeholders. With suitable modifications block chain can be adopted for cloud storage as reported in several research work. Several research works are ongoing to leverage the true potential power of the blockchain technology for cloud storage including “Google Drive, Dropbox, Gmail, etc”, The use of Cloud storage is exploding exponentially since large no. of users base is preferring to store their valuable data in cloud and ubiquitously admission their data and to get rid of risk of managing bundles of physical data or data in digital format. The companies namely Google, Microsoft and Amazon in the world including federals are leveraging benefits of the cloud computing. Therefore, it is necessary to look at improved quality of service (QoS) in the perspective of adding value by preserving private data, store in decentralized fashion with security principles.

References

[1] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M: A view of cloud computing. *Commun ACM* 2010, 53(4):50–58. 10.1145/1721654.1721672.

[2] Zhang Q, Cheng L, Boutaba R: Cloud computing: state-of-the-art and research challenges. *J Internet Serv Appl* 2010, 1(1):7–18. 10.1007/s13174-010-0007-6.

[3] Ardagna, D., Casale, G., Ciavotta, M. et al. Quality-of-service in cloud computing: modeling techniques and their applications. J Internet Serv Appl 5, 11 (2014). https://doi.org/10.1186/s13174-014-0011-3.

[4] Ardagna D, Panicucci B, Trubian M, Zhang L: Energy-aware autonomic resource allocation in multitier virtualized environments. *IEEE Trans Serv Comput* 2012, 5(1):2–19. 10.1109/TSC.2010.42.

[5] Prerita Gupta , Dr. Harmunish Taneja and Dr. Gagandeep Singh Brar , Quality of Services in Cloud Computing: Issues, Challenges and Analysis, ISSN : 2319-6319, International Journal of New Innovations in Engineering and Technology, Volume 3 Issue 3 – July 2015, page no. 76-81.

[6] Isaac Odun-Ayo, Member, IAENG, Olasupo Ajayi, and Adesola Falade, Cloud Computing and Quality of Service: Issues and Developments, Proceedings of the International MultiConference of Engineers and Computer Scientists 2018 Vol I, IMECS 2018, March 14-16, 2018, Hong Kong, ISBN: 978-988-14047-8-7, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online).

[7] Khan A, Yan X, Shu T, Anerousis N (2012) Workload characterization and prediction in the cloud: A multiple time series approach. In: Proceedings of the 2012 IEEE Network Operations and Management Symposium, NOMS 2012, 1287–1294, Maui, HI, USA.

[8] Di S, Kondo D, Walfredo C (2012) Host load prediction In a google compute cloud with a Bayesian model. In: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, SC12, 1–11, Salt Lake City, Utah, USA.

[9] Gmach D, Rolia J, Cherkasova L, Kemper A (2007) Workload analysis and demand prediction of enterprise data center applications. In: Proceedings of the 2007 IEEE 10th International Symposium on Workload Characterization, IISWC ’07, 171–180, Boston, MA, USA.

[10] Mattia Mrvosevic, Blockchain Based Decentralised Cloud Computing: Overview and Use Cases, https://medium.com/@eternacapital/blockchain-based-decentralised-cloud-computing-277f307611e1.

[11] Gartner, “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 21.4 Percent in 2018,” April 2018. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2018-04-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-21-percent-in-2018.

[12] Gartner, “Cloud Computing Tops List of Emerging Risks,” September 2018. [Online]. Available: https://www.gartner.com/smarterwithgartner/cloud-computing-tops-list-of-emerging-risks/.

[13] B. Schneier, “Should Companies Do Most of Their Computing in the Cloud?,” June 2015. [Online]. Available: https://www.schneier.com/blog/archives/2015/06/should_companie.html.

[14] Cloud Academy, “Disadvantages of Cloud Computing,” June 2018. [Online]. Available: https://cloudacademy.com/blog/disadvantages-of-cloud-computing/.

[15] IDC, “Worldwide Semiannual Internet of Things Spending Guide,”[Online]. Available: https://www.idc.com/getdoc.jsp?containerId=IDC_P29475.

[16] O. Vermesan and P. Friess, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems,” 2013. [Online]. Available: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf.

[17] F. Mattern and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich, 2010.
[18] CNN, "Your car's data may soon be more valuable than the car itself," February 2017. [Online]. Available: https://money.cnn.com/2017/02/07/technology/car-data-value/index.html.
[19] Cisco, "Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper," Cisco, 2018.
[20] Gartner, "Top 10 Technology Trends Impacting Infrastructure & Operations for 2018," December 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-10-technology-trends-impacting-infrastructure-operations-for-2018/.
[21] Information Age, "Moving from central to the edge: Is cloud decentralisation inevitable?," June 2018. [Online]. Available: https://www.information-age.com/cloud-decentralisation-inevitable-123472539/.
[22] Mimik, "As networks choke, edge cloud is the saviour," July 2017. [Online]. Available: https://mimik.com/as-network-chokes/.
[23] R. Brundo Uriarte and R. De Nicola, "Blockchain-Based Decentralised Cloud/Fog Solutions: Challenges, Opportunities and Standards," September 2018. [Online]. Available: https://www.researchgate.net/publication/326346449_Blockchain-Based_Decentralised_CloudFog_Solutions_Challenges_Opportunities_and_Standards.
[24] S. Ellis, A. Juels and S. Nazarov, "ChainLink — A Decentralized Oracle Network," September 2017. [Online]. Available: https://link.smartcontract.com/whitepaper.
[25] A. S. De Pedro, D. Levi and L. I. Cuende, "Witnet: A Decentralized Oracle Network Protocol," November 2017. [Online]. Available: https://witnet.io/static/witnet-whitepaper.pdf.
[26] The Future of Cloud Computing: Blockchain Will Have Its Day By Harsh Arora and Archi Bhatia on May 1, 2019, https://www.dataversity.net/the-future-of-cloud-computing-blockchain-will-have-its-day/
[27] C. Song, S. Wu, S. Liu, R. Fang and Q.-L. Li, "ANKR — Build a Faster, Cheaper, Securer cloud using idle processing power in data centers and edge devices," [Online]. Available: https://www.ankr.network/.
[28] T. Hanke, M. Movahedi and D. Williams, "Dfinity — The Internet Computer," [Online]. Available: https://dfinity.org/faq/.
[29] T. Hanke, M. Movahedi and D. Williams, "DFINITY Technology Overview Series — Consensus Mechanism," [Online]. Available: https://assets.ctfassets.net/ywqk17d3hsnp/2C8QU0x3q4AwuYYU4qiEmo/fb575987ca36672152a47b83ec96c0fc/dfinity-consensus.pdf.
[30] A. Yakovenko, "Solana: A new architecture for a high performance blockchain," [Online]. Available: https://solana.com/solana-whitepaper.pdf.

[31] Losavio, Michael and Pavel Pastukhov, and Svetlana Polyakova. "Regulatory Aspects of Cloud Computing in Business Environments." In Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments. edited by S. Srinivasan, 156-169. Hershey, PA: IGI Global, 2014. http://doi:10.4018/978-1-4666-5788-5.ch009.
[32] Gaetani, Edoardo, Aniello, Leonardo, Baldoni, Roberto, Lombardi, Federico, Margheri, Andrea and Sassone, Vladimiro (2017) Blockchain-based database to ensure data integrity in cloud computing environments. Italian Conference on Cybersecurity, Italy. 17 - 20 Jan 2017. 10 pp ., http://ceur-ws.org/Vol-1816/paper-15.pdf, PP.146-155, https://eprints.soton.ac.uk/411996/
[33] Mehdi Sookhak, Abdullah Gani, Hamid Talebian, Adnan Akhunzada, Samee U. Khan, Rajkumar Buyya, and Albert Y. Zomaya. Remote Data Auditing in Cloud Computing Environments: A Survey, Taxonomy, and Open Issues. ACM Comput. Surv., 47(4):65:1–65:34, May 2015.
[34] Gartner Says Worldwide IaaS Public Cloud Services Market Grew 37.3% in 2019, https://www.gartner.com/en/newsroom/press-releases/2020-08-10-gartner-says-worldwide-iaas-public-cloud-services-market-grew-37-point-3-percent-in-2019.
[35] Christy Pettey, Cloud Shift Impacts All IT arkets,https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets/,October 26, 2020
[36] Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, Viktor Niculichev, Lucas Yalansky Ensuring Data Integrity Using Blockchain Technology, PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION, 534-539,
[37] Deepak K. Tosh ,Sachin Shetty ,Xueping Liang ,Charles A. Kamhoua ,Kevin A. Kwiat and Laurent Njilla, Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack,Year: 2017, Volume: 1, Pages: 458-467, DOI Bookmark:10.1109/CCGRID.2017.111
[38] Amir Teshome, Sean Peisert, Louis Rilling, and Christine Morin, "Blockchain as a Trusted Component in Cloud SLA Verification", UCC '19 Companion, December 2–5, 2019, Auckland, New Zealand © 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM. ACM ISBN 978-1-4503-7044-8/19/12. . . $15.00 https://doi.org/10.1145/3368235.3368872, https://escholarship.org/content/qt2r60s6b5/qt2r60s6b5.pdf?t=q87lqj.
[39] Ghorbel, A., Ghorbel, M. & Jmaiel, M. Privacy in cloud computing environments: a survey and research challenges. *J Supercomput* **73,** 2763–2800 (2017). https://doi.org/10.1007/s11227-016-1953-y
[40] US Privacy Protection Study Commission (1977) Personal Privacy in an Information Society-the Report of the Privacy Protection Study Commission, https://epic.org/privacy/ppsc1977report/
[41] Directive EU (1995) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Off J EC 23(6), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.
[42] Bull G (2001) Data protection safe harbor: transferring personal data to the USA. Comput Law Secur Rev 17(4):239–243

[43] De Hert P, Papakonstantinou VN, Kamara I (2014) The new cloud computing ISO/IEC 27018 standard through the lens of

the EU legislation on data protection. It should be noted that privacy is worst in CC with many concerns and problems. The cloud service provider (CSP) is responsible for implementing privacy well within the framework of user requirements with legal standards.

[44] Anish Jaipuriar , Ashutosh Nagar , Varun Kalway and Sayantika Ganguly, India: Blockchain And Data Privacy: An India Perspective, 24 August 2020, https://www.mondaq.com/india/fin-tech/978488/blockchain-and-data-privacy-an-india-perspective.

[45]. Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, Keping Yu, AuthPrivacyChain: A Blockchain-Based Access Control Framework with Privacy Protection in Cloud, https://waseda.pure.elsevier.com/en/publications/authprivacychain-a-blockchain-based-access-control-framework-with.

[46] SPECIAL SECTION ON CLOUD - FOG - EDGE COMPUTING IN CYBER-PHYSICAL-SOCIAL SYSTEMS (CPSS) Received January 17, 2020, accepted January 27, 2020, date of publication January 30, 2020, date of current version February 10, 2020. Digital Object Identifier 10.1109/ACCESS.2020.2970576 Smart Contract Privacy Protection Using AI in Cyber-Physical Systems: Tools, Techniques and Challenges .

[47] https://juliankoh.medium.com/introduction-to-privacy-preserving-smart-contracts-e7bdc1a121b1. The different methods include Trusted Execution Environments (TEE).

[48] Chapter Six - Protecting personal sensitive data security in the cloud with blockchain, https://www.sciencedirect.com/science/article/pii/S006524582030084X

Dr.Arun kumar B.R.
Professor, Department of CSE,BMSITM, Bengaluru published nearly 70 research papers in national/international journals/conferences. He is working as reviewer /member of editorial board of several Journals including Scopus /WoS . He is serving as a Chairman, BOS, VTU MCA programme-2019-2022. He has delivered more than 50 expert talks, participated in nearly 100 FDPs, guided 5 M.Phil scholars and presently guiding 3 Ph.D scholars.