How to Cite:
Ramkrishna, S., Srinivas, C., Narasimhaiah, A. P., Muniraju, U., Maruthikumar, N. B., & Manjunath, R. I. (2022). A survey on blockchain security for cloud and IoT environment. International Journal of Health Sciences, 6(7), 28–43. https://doi.org/10.53730/ijhs.v6n7.10692

A survey on blockchain security for cloud and IoT environment

Shwetha Ramkrishna
Post Graduation Student, Master of Technology, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; E-mail:– shwetha.sit@gmail.com

Chetana Srinivas
Associate Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; Email:- chetanasrinivas2008@gmail.com

Achyutha Prasad Narasimhaiah
Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; Email:- achyuth001@gmail.com

Usha Muniraju
Assistant Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; Email:- usharaj.m@gmail.com

Nalini Bpalya Maruthikumar
Assistant Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; Email:- nalinibm03@gmail.com

Ramya Iyaravally Manjunath
Assistant Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, Karnataka, India; Pincode:- 560091; Email:- ramyaim31@gmail.com

***Abstract*---**In traditional Internet of Things (IoT) ecosystems, fog devices transmit data from sensors to a centralized cloud server. Issues with security and upkeep while updating firmware for millions of smart devices, single points of failure, as well as third-party Cloud server administration, the difficulty of frequently updating the firmware on millions of smart devices presents security and maintenance issues as well as a bottleneck in information flows, all raise privacy concerns. Blockchain technology eliminates the need for

trusted third parties while also preventing single points of failure and other issues. As a result, academics are looking into the usage of blockchain in the IoT space. The most recent state-of-the-art developments in blockchain for IoT, blockchain for Cloud, blockchain for eHealth, smart cities, transportation, and other programmes are examined in this article.

***Keywords*---**Blockchain technology, Cloud Data Security, Fog computing, Internet of Things.

Introduction

Academics, researchers, and businesses are all fascinated with the Internet of Things (IoT) way to its potential to provide revolutionary offerings throughout numerous programs. Because of its potential to give revolutionary offers across a variety of programmes, academics, researchers, and businesspeople are all interested in the Internet of Things (IoT). IoT has risen in importance, potential, and along with the advent of smart homes, smart cities, and other smart things; by 2020, it's predicted that there will be more than 50 billion connected gadgets. Many network technologies have been promoted in the literature as key components for the longer-term Internet of Things, such as Machine-to-Machine (M2M), Wireless Sensor Networks (WSNs), and Cyber-Physical Systems (CPS). As a result, with the standard IP community protocol, security concerns concerning WSN, M2M, or CPS develop in IoT, the need for comprehensive community security protection against security threats.

Criminal assaults, on the other hand, might stymie IoT solutions while also jeopardizing data security, user privacy, and network secrecy. However, blockchain, which was initially successfully deployed in cryptocurrencies, has the potential to be an extremely stable and for IoT applications, a privacy-preserving platform is available. This is shown in figure1.Blockchain is the technology that gives a steady manner to keep and manner statistics throughout a massive range of network participants. It's a decentralized tamper-proof, transactional database that enables central storage and sharing of massive amounts of data. In the present situation, an IoT system may bottleneck because of massive volumes of data from several IoT devices, which would lead to subpar service quality (QoS). Single factor of failure is a phrase that describes an issue with a machine that can interrupt the whole community from going for walks if it crashes. That's unwanted in any machine for attaining excessive availability and reliability book The Machine Whisperer. The peer-to-peer (P2P) structure of the blockchain appears to be a viable a solution to single point of failure and a bottleneck concerns.

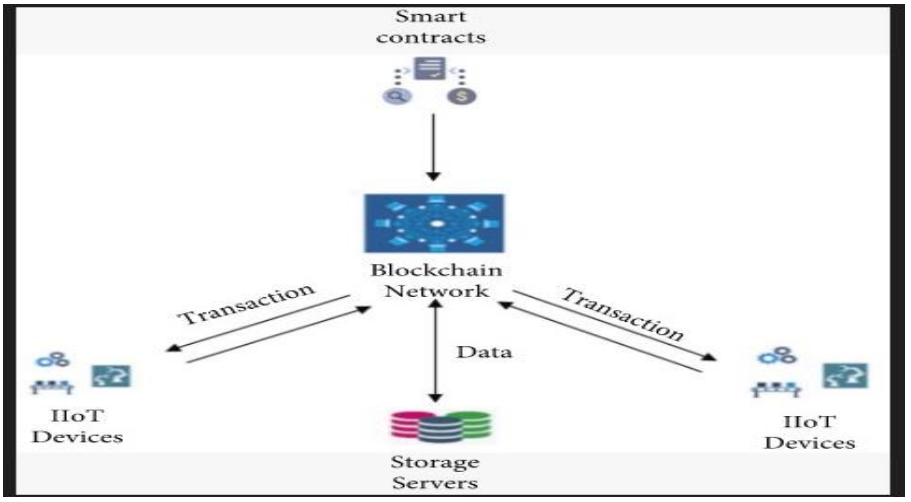

Fig1. Block Chain Network

Blockchain can remove a Internet of Things single point of failure and provide a reliable and efficient way to preserve and manage IoT records. Furthermore, the blockchain age has emerged as a critical treatment for reducing have faith in traditional government or, to put it more broadly, online intermediaries, because blockchain is supposed to do away with the necessity for trust between parties. In the blockchain era, members are more hesitant to accept the authority of a technological mechanism than they are to believe the authority of a centralizedorganization that may appear to have a bad reputation. Filippi et al. taken into account the fact that blockchain-based totally structures are supposed to instil faith in a selected machine, now no longer via way of means of absolutely doing away with believe, however instead by maximizing the degree of self belief among members as a way of in a roundabout way decreasing the want for believe. Blockchain lets in a circle of believe among unbiased events who do now no longer conform to trust solely on an outsider source of information. Technical solutions, in particular open-source applications, showing how the code of a particular piece of software can available to a certain level, make self-confidence or belief more easily carried out, the feasible final results may be greater easily anticipated theoretically. As a result, the software programme code's predictability improves, the more thought inside the machine, the less faith in the technical machine's builders or operators is required. Evidence of Work , a miner without utilising any monetary organisation or centralised authority. As a result, members of the Bitcoin community will produce a positive quantity of latest Bitcoins at the chosen rate (one block according to 10 min). No person can fake to be depended on, nor can a celebration be faked to make it seem like someone else is celebrating the event. Therefore, members of the community must trust that no person desires to be dependant on another person, and vice versa. This paper consciousness on rising protection technology which might be promising to offer protection for IoT programs withinside the (near) destiny. Cloud garage and blockchain technology offer secured disbursed databases for obvious and verifiable deployment, tool management. Post quantum cryptography gives equipment to steady gadgets towards destiny quantum assailants. By tackling related optimization tasks, evolutionary

algorithms are utilized to find answers to difficult security problems. According to the US Department of Homeland Security, the improvement of synthetic intelligence that controls the security of our IoT systems, including gadgets, data, pauses, and other things is linked to evolutionary processes, repairs devices in the case of a cyber-attack or other such incident.

Literature Survey

We asked people to fill out a survey, cognizance based on safety of IoT gadgets, merchandise, and technology. IoT gadgets have turn out to be one of the maximum not unusual place assault objectives for cybercriminals. A unexpectedly growing quantity of IoT gadgets acerbates those troubles even similarly. Between 2019 and 2030, it is predicted that by the year 2020, there will be 24.1 billion IoT-connected devices worldwide. These gadgets are designed to create hybrid networks that draw inspiration from the Internet of Things (IoT), smart grids, sensor networks, and other ideas.Because IoT devices must contend with issues such as low power, low potential, and limited performance, the authors of advocate for collaboration between IoT and cloud computing. The use of IoT devices in conjunction with cloud computing technology can lead to more efficient goods. In the idea of the Internet of cloud is mentioned. Procedures that are used in the past to the IoT cannot fulfill each needs of low value and simplicity; rather they have to balance the needs of high value and complexity. However, the cloud affords an answer with the capacity to fulfill each needs. Cloud computing can provide the IoT with an infinite supply of computing power, without problems on hand through the Internet, with higher resilience, and at a decrease value. Security is impacted by the convergence of cloud and IoT, as well as how devices interact with each other IoT adopting cloud computing has additionally delivered new safety demanding situations.

The safety components of IoT and cloud computing have been discussed in greater detail in more than one of the more recent articles.Some of the brand new and thrilling demanding situations on this vicinity are highlighted. Using cloud computing and the Internet of Things (IoT) together briefly discussed, with an emphasis on the security challenges that each technology faces. Despite the fact that cloud security is a well-known concern, combination of the cloud with the Internet of Things adds to the privacy and data security problems. Mobile cloud computing integrates the cloud computing era with mobile devices to improve processing power, memory, storage, strength, and situational awareness. They additionally join those regions with any other era, known as Mobile Cloud Computing (MCC). According to the principle safety troubles are an old OS and susceptible passwords and safety has now no longer usually been taken into consideration in product design, because of the concept of networking home equipment and different gadgets being exceptionally new. Embedded operating systems and software for IoT devices are frequently outdated and unpatched. Customers also commonly fail to modify the smart device's default password, or if they already do, they do not employ passwords that are sufficiently secure. IoT and cloud infrastructure security is becoming increasingly intertwined. According to the initial Internet of Things botnet was found in December 2013, With more than 25% of the botnet made up of non-PC gadgets like smart TVs, baby monitors, and other household appliances. Because there are so many various

technologies and systems in use in the IoT, it's challenging to create a unified safety policy.

Some gadgets in the Internet of Things (IoT) may no longer have enough computing potential and/or reminiscence for enforcing safety precautions. IoT gadgets are regularly powered via way of means of batteries with restricted potential and need to be shop strength. IoT gadgets are regularly powered via way of means of batteries with restricted potential and need to shop strength. Securing an IoT tool in opposition to a few kinds of assaults reasons massive will increase in strength consumption; therefore, it's far critical to first pick out feasible threats after which put into effect suitable countermeasures for the unique structure of the advanced IoT system.

Data Security using Block Chain

This section digs into the intricacies of blockchain technology as well as the challenges that occur when blockchain and IoT are combined (Internet of Things). The fundamentals of blockchain technology are as follows: furnished and accompanied through an element description of every factor, the goals of integrating blockchain technology with IoT defined and a few limitations set out in the definition of the term 'blockchain'. Wireless sensor networks can be used to build an eHealth framework, and in addition to Internet of Things, Cloud of Things, and blockchain generation, the study covered in this newsletter included smart houses. The Internet of Things (IoT), the Cloud of Things, and blockchain technologies are defined reviewing present studies from various domain names that included the technology cited above.

Basics of Block Chain Evolution

The generation of the Bitcoin cryptocurrency that Satoshi Nakamoto created in 2009, is known as blockchain. It is primarily described as the generation that underpins the 2009 invention of Satoshi Nakamoto's digital currency Bitcoin. This is shown in fig2. It is typically described as a decentralised, transparent, and trusted account on a P2P network. A transaction is the smallest unit of data on the blockchain, and positive numbers are grouped together to form a block, or chain. All the blocks that were shown are used to establish a decentralised blockchain ledger. A block in the allotted ledger is connected to a previously validated block using the cryptographic hash code. This next generation has already been thoroughly investigated in order to create a number of programmes outside virtual currency. Every player on a P2P community can confirm the attitude of different members withinside the community, in addition to make, confirm and approve a brand new transaction. This architecture offers secure and environmentally friendly blockchain processes having the added benefit of tamper resistance, additionally lowering the dangers of a single point of failure. Everyone has access to the blockchain ledger members however nonetheless now no longer regulated through any community authorities. The consensus mechanism is the procedure for synchronising the decentralised ledger across all blockchain nodes. This precept is completed through implementing strict policies and mutual settlement many of the community nodes, that is characterized because of the consensus mechanism in Bitcoin.

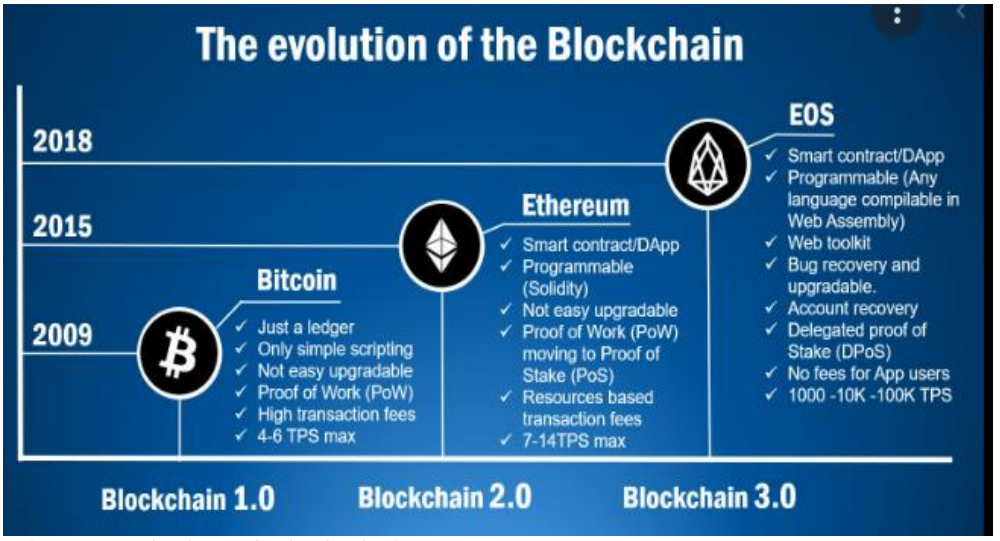

Fig 2 : Evolution of BlockChain

Description of the Blockchain Technology

There are numerous research articles available are divided blockchain technology into distinct tiers. The phase denotes the five layers that make up a blockchain generation, as well as study on the immutability, security, and integrity of the blockchain.

Objectives of blockchain technology in IoT

Blockchain technology's introduction has ushered in a new era of innovation offered a number of benefits to a variety of sectors in trustless situations[15], fifteen and delineated below Blockchain could be a viable method for identifying bottleneck and single-point failure concerns in the Internet of Things (IoT) industry. By doing so, it might be possible to do away with the requirement for an IoT network's dependable third party. Even if a few nodes go offline, the network's supply or security are not jeopardised. The failure of a node has no impact on the blockchain and IoT network's operation, moreover, the system is extremely resistant to both technological and malevolent attacks. Blockchain's peer-to-peer architecture grants all network users genuine validation privileges, allowing them to predict the accuracy of IoT data and guaranteeing immutability as shown in fig3. On the other hand, several ancient knowledgebase trust one or with a large number of servers, they're more vulnerable to cyber-attacks and technological failures. Enhanced Security: Compared to earlier record-keeping systems, blockchain is more reliable and secure in a number of ways. Instead of being held on a single server, transactions are logged over a network of computers, which prevents hackers from gaining access to transaction data. The use of PKI (private/public key infrastructure) is the most crucial component of security in blockchains. Asymmetrical cryptography is used to safeguard transactions between participants. Because these keys are generated using random integers and strings, a private key cannot be mathematically derived from its public key. Customers will have secure access control thanks to blockchain and IoT, which

will automatically authorise all IoT device actions.. This protects sensitive data from completely different applications as well as money services, government, and aid. It also has the potential to rework, although advice is offered to prevent fraud and bootlegging in any industry. Users can set access criteria for self-executing sensible contracts on the blockchain, ensuring privacy and non-public knowledge ownership. Additionally, smart contract services give consumers access to data sources, enabling owners of data to regulate the sharing of their data on blockchains. Improved traceability: In different systems, merchandise listed during a convoluted offer chain can't be duplicated back to its original purpose as quickly. Victimization smart contract-based authorisation can be used to verify and disable malicious access. Historical data transactions in blockchain will help ensure they are legitimate. A patient's prior medical data, which are essential to their care, can also be stored and tracked via the blockchain. Transparency: Blockchain might be a sort of distributed network within a regular network where all users share the same documents as essential individual copies. Because all or any network users may see the blockchain transaction histories they have far greater transparency and can be tampered with at any time. It suggests that of a consensus, that means that everybody must agree. To put it another way, the identical copy of blockchain knowledge is disseminated throughout a broad public validation network. As a result, all blockchain users will be affected have truthful rights to link, verify, and follow trading actions across the network. To change one transaction record, all following records must also be changed, necessitating network-wide collusion. As a result, information saved on a blockchain is significantly more accurate, reliable, and transparent than information maintained on a traditional network. This transparency also helps to ensure the integrity of blockchain-based systems by lowering the possibility of unauthorised data alterations. Knowledge Storage solutions on the blockchain are particularly cost-effective for securing IoT data from tampering due to blockchain's immutability and trustworthiness. Blockchain keeps track of data transfers and events in a way that guarantees authenticity and preserves integrity via immutable hash chains. In essence, the blockchain, on the other hand, allows customers to protect their computers and intellectual property while keeping track of network transactions. Reduced worth: One of the most common goals for many firms is to reduce costs. The necessity for third parties or middlemen is eliminated, as is the cost of preparing infrastructure for public blockchain, which may lower the value of operating company. Blockchain eliminates the need for middlemen or third parties, as well as the expense of infrastructure preparation for public blockchain, which may reduce the value of operational business. (For example, in the Ethereum blockchain, Gas). On the blockchain, there is no such thing as immutability, dealing knowledge is unchangeable throughout time. Technically, when a transaction is reviewed because of the blockchain network, it is timestamped and using a hashing process, they are arranged into a cryptographically safe block. Hash techniques connect blocks to form a chain. The previous block's hash value is maintained indefinitely in one field in the header of a new block, making the chain powerfully immutable. When the block data is genuine and recorded inthe blockchain, it can't be modified, edited, or erased in this way. Any attempts to alter or modify transactions will be met with the cryptological link between succeeding blocks. Any modifications that occur during the course of a transaction will be clearly visible.

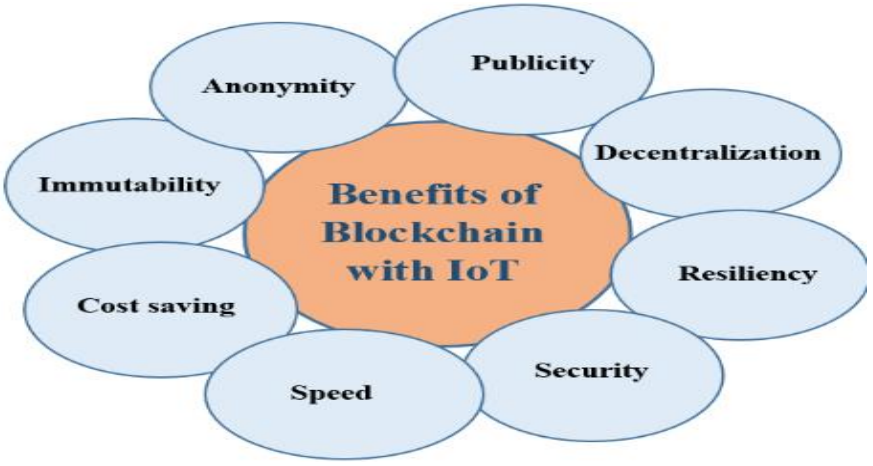

Fig 3: Benefits of blockchain with IoT

Blockchain and Internet of Things

A centralised server, typically a cloud server, thanks to the Internet of Things (IoT), which connects people, things, and goods, gets data through embedded microprocessors, sensors, and actuators. IoT analytics tools use data from IoT devices to create concepts, observe Contribute to innovative services and business processes. However, the IoT scheme's security and privacy are major factors that have hampered its development on a larger scale. Security issues, such as DDOS, Ransom ware, and malicious assaults, are common in IoT networks DDoS is a sort of attack in which a target, a central server, for example, is inundated with synchronic information requests from a large number of infected computers, resulting in network users being denied service. Furthermore, as the quantity of gadgets that need to be authenticated, approved, and connected to an IoT network grows, existing centralised systems will face a bottleneck problem when adding new nodes to the network by authenticating, approving, and joining them to the network. As a result of the proposed solutions to the aforementioned IoT challenges, blockchain, often referred to as DTL, has shown, as a game-changing technology that will likely address a range of IoT security and privacy issues, and quantifiability issues. The blockchain's distributed ledger might be tamper-resistant, removing the need for trust between the people concerned Smart cities, smart infrastructure, smart grids, smart transportation, smart homes, and smart healthcare systems are all examples of IoT applications. The preparation of blockchain in the IoT domain has resulted in the creation of BCIoT, a substitute blockchain domain for IoT. No single entity is in charge of the massive amounts of information produced by IoT devices under the BCIoT paradigm. In addition, blockchain technology allows parties to keep track of previous transactions. As a result, data leakage is rapidly recognized and repaired. Because IoT ASCII text files are held on by web third parties and telecommunications carriers, ensuring integrity has become a critical analysis issue in IoT applications, resulting in a lack of confidence among users. A variety of factors influence the utility of blockchain in an IoT network:

(1) If an Internet of Things (IoT) application intends to create a decentralised Peer-to-Peer environment, blockchain will provide a solution to the privacy and security concerns.
(2) Blockchain may provide a viable and safe solution for an IoT application that wants to retain a payment method for its offered services without relying on third-party management.
(3) One of the most effective options could be the blockchain. for IoT applications that require logs and traceability of ordered transactions.

When creating an IoT device architecture that works with a blockchain ledger, however, there are some significant challenges to solve.
(1) Managing the large volumes of data collected by various IoT devices on-chain is one of the main issues with combining blockchain with IoT. Furthermore, when processing group operations, the blockchain is likely to experience slower speeds or higher latency.
(2) Another important consideration is maintaining network privacy and transaction confidentiality: in a public blockchain, transaction history anonymity cannot be guaranteed. By analysing transaction patterns, attackers will be able to identify the identities of people or devices.

Blockchain and Cloud

In order to streamline data collection and provide users with quality of service (QoS), an important number of Electronic Medical Records (EMRs) are being produced and traded between people and healthcare organizations as digital healthcare usage increases. Cloud computing, , specifically, offers strong health data sharing services, such as the processing of Electronic Health Records (EHRs) patients use mobile devices to access data stored on cloud servers. IoT paired with Cloud computing allows for on-demand treatment, saves medical costs, and improves customer satisfaction. On the other hand, information sharing in the Cloud is at danger due to the possibility of hostile assaults and a dearth of confidence between cloud storage providers, cloud suppliers, and users. This compromises the network and endangers the medical service, and it also causes major data leakage. The problems that have been raised in Cloud ecosystems while transmitting health data will be addressed by blockchain technology, which has great immutability, stability, and trust worthiness alternatives. Blockchain, in particular strong blockchain contracts, can improve safe data transmission in Cloud IoT-enabled support networks, where blockchain and the cloud are key players in regulating user access and data sharing, can change the prominence and authenticity of any record on the blockchain, providing safety and defense for unreliable aid settings as shown in fig 4. Blockchain models encourage patients and healthcare institutions should work together to defend data security and privacy. The inclusion cloud computing and blockchain technology will vastly increase the security of cloud eHealth storage services.

Fig 4: Blockchain and Cloud

Under blockchain governance, using cloud storage, peers in a peer-to-peer network. Several researchers recommend encrypting health data and keeping it in traditional Cloud storage while also putting the data's produced hash code on the blockchain, it enables knowledge traceability and promptly recognizes the hazards of cloud data sterilization. Health care services will be specialized, incredibly trustworthy, and productive thanks to blockchain. Clinical services include health monitoring, patient diagnosis, and evaluation of medical interventions, could be reworked with blockchain. As a result, implementing blockchain models in the healthcare business has the potential to improve patient service while also ensuring system security.

Conclusion

To address security and privacy concerns, this paper combined IoT, Cloud computing, and blockchain technology. Despite this, there are a number of technological and security challenges with the IoT that have yet to be resolved. Several issues in enterprise blockchain technology within the IoT area are covered in this review paper, as well as how they are being solved. To analyze the merits and limits of existing blockchain and IoT articles, a range of criteria are used to assess them.

Acknowledgments

I extend my deep sense of sincere gratitude to Dr. Channakesavalu K, Principal, East West Institute of Technology, Bengaluru, for having permitted to carry out the survey on “A Survey on Blockchain Security for Cloud and IoT Environment” successfully.

I express my heartfelt sincere gratitude to my guide Prof. Chetana Srinivas, Associate Professor, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru for his valuable guidance, encouragement and suggestions.

I express my heartfelt sincere gratitude to Dr. Achyutha Prasad N, Professor & Head, Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru for his valuable guidance, encouragement and suggestions.

I would like to thank all the Teaching, Technical faculty and supporting staff members of Department of Computer Science and Engineering, East West Institute of Technology, Bengaluru, for their valuable suggestions and support.

Finally, I would like to thank my Parents for their support.

References

1. D.C. Nguyen, P.N. Pathirana, M. Ding, et al., Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges, arXiv, 2019. preprint.
2. F. Ellouze, G. Fersi, M. Jmaiel, Blockchain for internet of medical things: a technical review, in: M. Jmaiel, M. Mokhtari, B. Abdulrazak, et al. (Eds.), The Impact of Digital Technologies on Public Health in Developed and Developing Countries, vol. 12157, Springer, Cham, France, 2020, pp. 259–267.
3. M.H. ur Rehman, I. Yaqoob, K. Salah, et al., The role of big data analytics in industrial internet of things, Future Generat. Comput. Syst. 99 (2019) 247–259.
4. S.S. Panda, U. Satapathy, B.K. Mohanta, et al., A blockchain based decentralized authentication framework for resource constrained IoT devices, in: 2019 10th International Conference on Computing, Communication and Networking Technologies; 6–8 Jul 2019; Kanpur, India, IEEE, Piscataway, NJ, USA, 2019, pp. 1–6.
5. M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Generat. Comput. Syst. 82 (2018) 395–411.
6. N. Siegfried, T. Rosenthal, A. Benlian, et al., Blockchain and the Industrial Internet of Things: A Requirement Taxonomy and Systematic Fit Analysis, Publications of Darmstadt Technical University, Institute for Business Studies, 2020, p. 117408.
7. R.A. Michelin, A. Dorri, M. Steger, et al., Speedychain: a framework for decoupling data from blockchain for smart cities, in: 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services; 5–7 Nov 2018; New York, NY, USA, ACM, New York, NY, USA, 2018, pp. 145–154.
8. Y. Yu, Y.N. Li, J.F. Tian, et al., Blockchain-based solutions to security and privacy issues in the internet of things, IEEE Wireless Communications 25 (6) (2018) 12–18.
9. Panarello, N. Tapas, G. Merlino, et al Blockchain and IoT integration: a systematic survey. Sensors. 18(8)(2018): 2575.
10. J.Q. Huang, L.H. Kong, G.H. Chen, et al., towards secure industrial IoT: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inform. 15 (6) (2019) 3680–3689.
11. Q.H. Zhou, H.W. Huang, Z.B. Zheng, et al., Solutions to scalability of blockchain: a survey, IEEE Access 8 (2020) 16440–16455.
12. P.P. Ray, D. Dash, K. Salah, et al., Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases, IEEE Syst. J. 15 (1) (2020) 85–94.
13. P. de Filippi, M. Mannan, W. Reijers, Blockchain as a confidence machine: the problem of trust & challenges of governance, Technol. Soc. 62 (2020) 101284.

14. A. Antonopoulos, Bitcoin Security Model: Trust by Computation. use Bitcoinsinfo, 2014. Available online, https://usebitcoins.info/index.php/news/2460-bitcoin -security-model. (Accessed 4 October 2015).
15. K.R. Ozy € ılmaz, A. Yurdakul, Work-in-progress: integrating low-power IoT devices to a blockchain-based infrastructure, in: 2017 International Conference on Embedded Software; 15–20 Oct 2017; Seoul, Republic of Korea, IEEE, Piscataway, NJ, USA, 2017, pp. 1–2.
16. K.J. O'Dwyer, D. Malone, Bitcoin mining and its energy footprint, in: 25th IET Irish Signals & Systems Conference 2014 and 2014 China–Ireland International Conference on Information and Communications Technologies; 26–27 Jun 2014; Limerick, Ireland, IET, London, 2014, pp. 280–285.
17. M.A. Uddin, A. Stranieri, I. Gondal, et al., An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring, in: 2019 IEEE International Conference on Industrial Technology; 13–15 Feb 2019; Melbourne, Australia. Piscataway, IEEE, NJ, USA, 2019, pp. 1135–1142.
18. P.K. Sharma, N. Kumar, J.H. Park, Blockchain technology toward green IoT: opportunities and challenges, IEEE Network 34 (4) (2020) 263–269.
19. A.D. Dwivedi, L. Malina, P. Dzurenda, et al., Optimized blockchain model for Internet of Things based healthcare applications, in: 2019 42nd International Conference on Telecommunications and Signal Processing; 1–3 Jul 2019; Budapest, Hungary, IEEE, Piscataway, NJ, USA, 2019, pp. 135–139.
20. H.F. Atlam, G.B. Wills, Technical aspects of blockchain and IoT, in: S. Kim, G.C. Deka, P. Zhang (Eds.), Advances in Computers, vol. 115, Elsevier, Amsterdam, The Netherlands, 2019, pp. 1–39.
21. E. Karafiloski, A. Mishev, Blockchain solutions for big data challenges: a literature review, in: IEEE EUROCON 2017—17th International Conference on Smart Technologies; 6–8 Jul 2017; Ohrid, Macedonia, IEEE, Piscataway, NJ, USA, 2017, pp. 763–768.
22. Kyle, Blockchain issues: #1: Data storage, 2018. Available Online, https://medium.com/@Kyle.May/blockchain-issues-1-data-storage. (Accessed 5 April 2020).
23. T.X. Yu, X.B. Wang, Y.X. Zhu, Blockchain technology for the 5G—enabled internet of things systems: principle, applications and challenges, in: 5G—Enabled Internet of Things, CRC Press, Boca Raton, FL, USA, 2019.
24. J. Ellul, J. Galea, M. Ganado, et al., Regulating blockchain, dlt and smart contracts: a technology regulator's perspective, ERA Forum 21 (2) (2020) 209–220, 21.
25. A. Reyna, C. Martin, J. Chen, et al., on blockchain and its integration with IoT. Challenges and opportunities, Future Generat. Comput. Syst. 88 (2018) 173–190.
26. J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, J. Netw. Comput. Appl. 149 (2020) 102481.
27. Q. Feng, D. He, S. Zeadally, et al., A survey on privacy protection in blockchain system, J. Netw. Comput. Appl. 126 (2019) 45–58.
28. Q. Zhu, S.W. Loke, R. Trujillo-Rasua, et al., Applications of distributed ledger technologies to the internet of things: a survey, ACM Comput. Surv. 52 (6) (2019) 1–34.

29. W.B. Chen, Z.Y. Xu, S.Y. Shi, et al., A survey of blockchain applications in different domains, in: 2018 International Conference on Blockchain Technology and Application; 10–12 Dec 2018; Xi'an, China, ACM, New York, NY, USA, 2018, pp. 17–21.
30. A. Miglani, N. Kumar, V. Chamola, et al., Blockchain for internet of energy management: review, solutions, and challenges, Comput. Commun. 151 (2020) 395–41.
31. Piyush Kumar Pareek et al, 'Survey on Challenges in Devops ', International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-4, Issue-5, September-2016.
32. Dr.Piyush Kumar Pareek et al, 'Education Data Mining –Perspectives of Engineering Students ', International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-4, Issue-5, September-2016.
33. Dr.Piyush Kumar Pareek et al, 'A survey on approaches for predicting performance of students',International Journal of Engineering Research and Science, ISSN No.2395-6992 Paper Id:IJOER-Jun-2016-25.
34. Dr.Piyush Kumar Pareek et al, 'A survey on Long term product planning and requirements prioritization to customer value creation', International Journal of Engineering Research and Science, ISSN No.2395-6992 Paper Id: IJOER-Jun-2016-27.
35. Dr.Balakrishna R, Piyush Kumar Pareek et al, 'Study on Six Sigma approach to improve the quality of process outputs in business processes in Small & Medium Level Software Firms' Springer AISC Series/ SCOUPS INDEXED JOURNAL, Paper Id : IT -221-ICPCIT2015.
36. Dr.Balakrishna R, Piyush Kumar Pareek et al, 'Data Mining for Healthy Tomorrow with the implementation of Software Project Management technique', Springer AISC Series/ SCOUPS INDEXED JOURNAL, Paper Id : IT -187-ICPCIT2015, June 2015.
37. Piyush Kumar Pareek & Dr. A. N. Nandakumar, 'To Implement Lean software development frame- work for minimizing waste in terms of non-value added activities', Research Publishing, Jain University ICISTSI-15 , Innovative Partners for Publishing Solutions, Singapore (May 2015).
38. Piyush Kumar Pareek & Dr.A.N.Nandakumar, 'Identifying Wastes in software, International Journal of Engineering Studies and Technical Approach'. January Issue 2015.
39. Piyush Kumar Pareek & Dr.A.N.Nandakumar, 'Failure Mode Effective Analysis of Requirements Phase in small software Firms', Paper ID: ICSTM/YMCA/2015/292, International Conference on Science, Technology and Management (ICSTM-2015). International Journal of Advance Research in Science and Engineering (IJARSE, ISSN- 2319-8354, Impact Factor- 1.142) [www.ijarse.com], Special Issue Jan2015.
40. Mr. Piyush Kumar Pareek, Dr. A. N. Nandakumar, Lean software development Survey on Agile and Lean usage in small and medium level firms in Bangalore, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 12, December 2014 , ISSN: 2277 128X .pp 1-7 Impact Factor : 2.08.
41. Mr.Piyush Kumar Pareek, Dr. A. N. Nandakumar, 'Lean software development Survey on Benefits and challenges in Agile and Lean usage in small and medium level firms in Bangalore' , International Journal of Advanced

Research in Computer Science and Software Engineering , Volume 4, Issue 12, December 2014 , ISSN: 2277 128X .pp 1-11.

42. Piyush Kumar Pareek , Dr.Praveen Gowda , et al 'Ergonomics in a Foundry in Bangalore to improve productivity',International Journal of Engineering and Social Science , ISSN: 2249- 9482 ,Volume 2,Issue 5 (May 2012) , pp 1-6.
43. Piyush Kumar Pareek, Dr. Vasanth Kumar S A , et al 'Reduction of Cycle Time By Implementation of a Lean Model Carried Out In a Manufacturing Industry', International Journal of Engineering and Social Science , ISSN: 2249- 9482,Volume 2, Issue 5, pp 114-123.
44. Piyush Kumar Pareek , Dr.Praveen Gowda, et al 'FMEA Implementation in a Foundry in Ban- galore to Improve Quality and Reliability', International Journal of Mechanical Engineering and Robotics Research, ISSN :2278-0149,Volume 1,Issue 2(June 2012),pp 81-87.
45. Piyush Kumar Pareek, Dr.Vasanth Kumar S A , et al 'Implementation of a Lean Model for Carrying out Value Stream Mapping in a Manufacturing Industry', International Journal of Mechanical Engineering and Robotics Research, ISSN :2278-0149,Volume 1,Issue 2(June 2012),pp 88-95.
46. Piyush Kumar Pareek, Dr. A. N. Nandakumar, et al 'Methodology and Functioning of Project Management Techniques in Agile Software Development Process', International Journal of Research in IT, Management and Engineering, ISSN: 2249-1619, Volume2, Issue12 (December2012), pp 76-85.
47. N. A. Prasad and C. D. Guruprakash, "An ephemeral investigation on energy proficiency mechanisms in WSN," 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Tumkur, 2017, pp. 180-185.
48. A. P. N and C. D. Guruprakash, "A Relay Node Scheme for Energy Redeemable and Network Lifespan Enhancement," 2018 4th International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Mangalore, India, 2018, pp. 266-274.
49. Achyutha Prasad, N., Guruprakash, C.D., 2019. A relay node scheme of energy redeemable and network lifespan enhancement for wireless sensor networks and its analysis with standard channel models. International Journal of Innovative Technology and Exploring Engineering 8, 605–612.
50. Achyutha Prasad, N., Guruprakash, C.D., 2019. A relay mote wheeze for energy saving and network longevity enhancement in WSN. International Journal of Recent Technology and Engineering 8, 8220–8227. doi:10.35940/ijrte.C6707.
51. Achyutha Prasad, N., Guruprakash, C.D., 2019. A two hop relay battery aware mote scheme for energy redeemable and network lifespan improvement in WSN. International Journal of Engineering and Advanced Technology 9, 4785–4791. doi:10.35940/ijeat.A2204.109119.
52. Rekha VS, Siddaraju., "An Ephemeral Analysis on Network Lifetime Improvement Techniques for Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering, vol. 8, issue 9, 2278-3075, pp. 810–814, 2019.
53. Prasad N. Achyutha, Sushovan Chaudhury, Subhas Chandra Bose, Rajnish Kler, Jyoti Surve, Karthikeyan Kaliyaperumal, "User Classification and Stock Market-Based Recommendation Engine Based on Machine Learning and

Twitter Analysis", Mathematical Problems in Engineering, vol. 2022, Article ID 4644855, 9 pages, 2022. https://doi.org/10.1155/2022/4644855.

54. Achyutha, P. N., Hebbale, S., & Vani, V. (2022). Real time COVID-19 facemask detection using deep learning. International Journal of Health Sciences, 6(S4), 1446–1462. https://doi.org/10.53730/ijhs.v6nS4.6231.
55. Kalshetty, J. N., Achyutha Prasad, N., Mirani, D., Kumar, H., & Dhingra, H. (2022). Heart health prediction using web application. International Journal of Health Sciences, 6(S2), 5571–5578. https://doi.org/10.53730/ijhs.v6nS2.6479.
56. R. V S and Siddaraju, "Defective Motes Uncovering and Retrieval for Optimized Network," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 2022, pp. 303-313, doi: 10.1109/ICCMC53470.2022.9754109.
57. N. G and G. C. D, "Unsupervised Machine Learning Based Group Head Selection and Data Collection Technique," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 2022, pp. 1183-1190, doi: 10.1109/ICCMC53470.2022.9753995.
58. Jipeng, T., Neelagar, M. B., & Rekha, V. S. (2021). Design of an embedded control scheme for control of remote appliances. Journal of Advanced Research in Instrumentation and Control Engineering, 7(3 & 4), 5-8.
59. Chetana Srinivas, Nandini Prasad K. S., Mohammed Zakariah, Yousef Ajmi Alothaibi , Kamran Shaukat , B. Partibane, and Halifa Awal, “Deep Transfer Learning Approaches in Performance Analysis of Brain Tumor Classification Using MRI Images”, Hindawi Journal of Healthcare Engineering Volume 2022, Article ID 3264367, 17 pages https://doi.org/10.1155/2022/3264367.
60. Chetana Srinivas, Nandini Prasad K S,"A Comparative study on Medical Image Processing Using Big Data Analytics Frameworks”, 2018 Third International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, 2018.
61. Chetana Srinivas, Nandini Prasad K S,” A Comparative Study on Different Types of Image Pre-processing Methods for Noise Removal”, Internal Journal of Computing, Communication & Networking (IJCCN), ISBN: 2319-2720, Vol.7, Issue 2, April 2018.
62. Chetana Srinivas, Ambrish G, Bharathi Ganesh, Anitha Ganesh, Dhanraj, Kiran M, “Logistic Regression Technique for Prediction of Cardiovascular Disease”, International Conference on Intelligent Engineering Approach,(ICIEA) India, 12th February 2022.
63. Chetana Srinivas, Ambrish G, Supritha N, Bharathi G, Anitha G, “Survey on Recent Trends in Machine Learning and Deep Learning in Healthcare”, International Conference on Recent Trends in Machine Learning and Computing System,(RTMCS) India, 17th -18th December 2021.
64. Kadakadiyavar, S., Prasad, A. N., Pareek, P. K., Vani, V., Rekha, V. S., & Nirmala, G. (2022). Recognition efficiency enhancement of control chart pattern using ensemble MLP neural network. International Journal of Health Sciences, 6(S3), 4295–4306. https://doi.org/10.53730/ijhs.v6nS3.6851.
65. Manjunatha Kumar, B. H., Achyutha , P. N., Kalashetty, J. N., Rekha, V. S., & Nirmala, G. (2022). Business analysis and modelling of flight delays using artificial intelligence. International Journal of Health Sciences, 6(S1), 7897–7908. https://doi.org/10.53730/ijhs.v6nS1.6735.

66. Hebbale, S., Marndi, A., Manjunatha Kumar, B. H., Mohan, B. R. ., Achyutha, P. N., & Pareek, P. K. (2022). A survey on automated medical image classification using deep learning. International Journal of Health Sciences, 6(S1), 7850–7865. https://doi.org/10.53730/ijhs.v6nS1.6791.
67. Pooja Chopra, Vijay Suresh Gollamandala, Ahmed Najat Ahmed, S. B. G. Tilak Babu, Chamandeep Kaur, N. Achyutha Prasad, Stephen Jeswinde Nuagah, " Automated Registration of Multiangle SAR Images Using Artificial Intelligence & quot, Mobile Information Systems, vol. 2022, Article ID 4545139, 10 pages, 2022. https://doi.org/10.1155/2022/4545139.
68. Hebbale, S., Marndi, A., Achyutha, P. N., Manjula, G., Mohan, B. R., & Jagadeesh, B. N. (2022). Automated medical image classification using deep learning. International Journal of Health Sciences, 6(S5), 1650–1667. https://doi.org/10.53730/ijhs.v6nS5.9153.
69. Sagar, Y.S. and Achyutha Prasad, N., CHARM: A Cost-Efficient Multi-Cloud Data Hosting Scheme With High Availability, International Journal for Technological Research In Engineering, Volume 5, Issue 10, June-2018, ISSN (Online): 2347 – 4718.
70. Udit Shinghal, Yashwanth A V Mowdhgalya, Vaibhav Tiwari, Achyutha Prasad N "Centaur - A Self-Driving Car" International Journal of Computer Trends and Technology 68.4 (2020):129-131.
71. Udit Shinghal, Yashwanth A V Mowdhgalya, Vaibhav Tiwari, Achyutha Prasad N "Home Automation using HTTP and MQTT Server" International Journal of Computer Trends and Technology 68.4 (2020):126-128.
72. Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2021). Get vaccinated when it is your turn and follow the local guidelines. *International Journal of Health Sciences*, *5*(3), x-xv. https://doi.org/10.53730/ijhs.v5n3.2938