International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 08 | Aug 2021 www.irjet.net p-ISSN: 2395-0072

A Study of Blockchain-Based Cryptosystems with and without a Software Defined Network

Thyagarajamurthy A[1], Anusha M[2]

[1]Associate Professor, JSS-STU, Mysore, India
[2]PG Scholar, JSS-STU, Mysore, India

Abstract - *Networking, security, encryption standards, and communications are all important aspects of today's growing technology. When cryptosystems are employed to put up Blockchain-based systems, the survey highlights how software defined networks help to acquire security. How various cryptosystem algorithms such as DES, AES, SHA, Blowfish, and others play diverse roles in Blockchain. How each algorithm aids in the attainment of security, as well as its shortcomings when not implemented in SDN When compared to other algorithms, the DES algorithm plays a vital role in terms of energy efficiency, power consumption, data transaction, confidentiality, anonymity, authentication, and authorisation when Blockchain is applied in a Software Defined Network. SDN could be used to perform security attack tracing and node failure detection in the future. Nowadays, there are tremendous aspects in the fields of cyber security, transparency, and data monitoring. In this study, we looked at some of the upcoming solutions that experts have created to address network performance challenges. To begin, we'll go through the parameters that go into evaluating Blockchain performance, and then we'll go over how to improve the technology by using different encryption standards to get better performance. Finally, we came to a conclusion with positive results and the limitations of all of the major technologies and algorithms enclosed.*

Key Words: **Blockchain, Cryptosystem, Encryption Standards, Software Defined Network, Security, Privacy**.

1.INTRODUCTION

Crypto currency, which is a type of technology with several privacy capabilities, is a well-known factor in the current technology sphere. Because it relies entirely on cryptographic techniques. This is a distributed/decentralized technique that adheres to consensus rules and maintains a non-modifiable ledger to store transaction history. The data in blockchains is pre-stored in the form of a ledger, which is divided into blocks, each of which contains hash data and transaction details. Every block in the blockchain system is linked to the next in the form of blocks, making data manipulation virtually impossible.The few resolution algorithms examine and check data on all transactions within the blocks, guaranteeing that every event is accurate and genuine. Distributed ledger technology facilitates decentralisation by allowing people to collaborate in a decentralised network. There are hardly any points of vulnerability, as the activity log should therefore be changed by one user. However, the blockchain and comparable platforms have some important safety concerns. Who may engage in blockchain networks and who has access to the data can vary. Public or private networks are often branded as public or private, indicating who is permitted to participate, and permissioned or permissionless, indicating how users acquire access to the network. The blockchain is a distributed ledger that is similar to the linked list data structure format. However, the blockchain is distributed, whereas linked lists are pointers oriented.

Software-Defined Networking (SDN) is a new networking architecture trend that is dynamic, controllable, cost-effective, and flexible, making it ideal for today's high-bandwidth, real-time applications. The controller manages network control and forwarding, and in the event that the networking nodes are damaged, the controller chooses the shortest path, allowing network management to be directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow protocol is a key component in the development of SDN solutions. There are two types of encryption used in today's world: homogeneous and unsymmetrical encryption. The term stems from the fact that a single identifier is used for both encryption and decryption.

DES, AES, and RSA are the three main encryption types. While there are other types of encryption, far more than can be easily explained here, we will focus on the three most common types of encryption used by customers.According to the study, we are attempting to illustrate how blockchain plays a significant part in today's networking environment. by utilising SDN and the security role that this network performs in the field of privacy and security. What role does the DES algorithm play in SDN? This is used to determine how node failure happens and how an attack is traced.

2. MAJOR TERMS AND PHRASES

In order to provide a comprehensive understanding of the techniques and research, we provide a brief overview of the important scientific terms utilised in these selected survey papers in this part.

2.1 Software-defined networking (SDN)

Software-defined networking (SDN) is a networking technique that communicates with the underlying physical infrastructure and distributes congestion on a network using application controllers or application programming interfaces (APIs). Instead of (or in parallel with) conventional routers and switches, the SDN layer serves as a virtual software switch or router. As a result, rather than congestion management software inherent in routers and switches, technology from elsewhere takes significant over. SDN allows network professionals to direct communication channels and strategically arrange virtual networks by allowing users to supply new connections using software rather than physical infrastructure. SDN, unlike traditional switches, may also connect more effectively with networked devices.

2.2 Blockchain Technology

Bitcoin is a system for storing data that makes it difficult or hard to change, corrupt, or deceive. A blockchain is a distributed record track of actions that have been duplicated and disseminated all over the number of distributed servers that make up the blockchain. Simply said, blockchain technology is a decentralised, distributed ledger that tracks the ownership of various content. The data on a blockchain can't be changed by nature, making it a real disruptor in industries like transactions, information security, and medicine. Blockchain is a superior, secure visual representation of events and authorized users updated even while preserving the past. We get a statistical data trace as well as a promptly right-up record, and the content can't be altered or unintentionally erased. Blockchain is the technology that allows cryptocurrencies to exist (among several other things). A Bitcoin, like the US dollar, is a virtual form of currency that uses encryption skills to regulate the generation of national currencies and authenticate the transmission of payments.

2.3 Cryptosystem Standards

A cryptosystem is a collection of block ciphers used to provide a certain intelligence service, most typically to ensure anonymity (encryption). An encryption algorithm mainly consists of three algorithms: one for key creation, encoding, and decoding. It provides information to the intelligence community by implementing encryption methods using various cryptographic aspects, such as encrypted form, symmetric encryption, raw text, decryption of the data, and private keys. Symmetric Cryptographic Encryption and Asymmetric Encryption Authentication are two different types of cryptosystems.Encryption is a way of embedding information (messages or files) so that it can only be viewed or reported to the appropriate people. Crypto algorithms intercept data transferred over the internet using complicated algorithms. The content can be deciphered using a code provided by the message's author once it has been received.

2.4 Cryptography

The research into encrypted communications techniques that allow only the transmitter and intended destination of a document to read its contents is known as cryptography. Encrypting and decrypting email and other pure messages is perhaps the most prevalent usage of cryptography when transporting electronic data.Kryptos and logos are the two components of cryptology. Verification, information validation such as privacy and integrity, non-repudiation of authenticity, and anonymity are the key objectives of cryptosystems, which have two components: encoding and decoding. Secret-key encryption, public-key encryption, and hash function encryption are the three forms of cryptographic algorithms.

2.5 Data Encryption Standard (DES)

DES is an encryption algorithm that secures files in form of blocks. This implies that data of each of 64 bits of plain text are fed into DES, which generates entire bits of encrypted data. Encrypt and decrypt employ certain techniques and information, with slight variations. The key is 56 bits long. Encrypting sets of 64 cipher text, or 16 hexa integers, is how DES works. DES uses "values" that are purportedly 16 hexadecimal values long, or 64 bits. In contrast, the DES algorithm eliminates each 8th key bit, culminating in a block cipher of 56 bits.

2.6 Advanced Encryption Standard (AES)

AES is a secure method that encrypts and decrypts using the same 128, 192, or 256-bit key (the security of an AES system increases exponentially with key length). To examine AES's overall structure, with a focus on the four procedures utilised in each round: (1) byte replacement, (2) shifting rows, (3) mixing columns, and (4) adding round keys.

2.7 Digital Signature

A digital signature ensures that the intended message is not tampered with while on route. Whenever the service securely signs the document, the user uses the secret key to add a one-way hash (encryption) of the authentication tokens. Biometrics works by proving that a piece of electronic information or a file has not been tampered with after it has been signed, either knowingly or unknowingly. Digital signatures do this by generating a distinctive response message or content and encrypting it with the recipient's master password.

3. LITERATURE REVIEW

We attempt to offer a comprehensive review of all current modern research trends that have been conducted to evaluate the performance of blockchain technology in conjunction with various cryptosystem standards in the network area and other models below.

Manisha Nehe et al [1] proposes the major concerns about information security are identity, privacy, and exchange security. Data transparency, intensification of change, and fine-grained access to data information are all important features of block-chain technology, which is designed for data operational businesses that deal with vast amounts of sensitive data and are subject to frequent hacker attacks. This strategy allows for the adoption of a new blockchain architecture since data will be accessed by private and public key users, while network access will be improved through authorised keys based on the blockchain hash value.

Dr. V. Suma et al [2] since blockchain is a foundation technology, it draws a wide range of APIs that help to ensure secure data transactions across the network. The study also discusses how to use block chain to prevent misuse and corruption in the exchange of large amounts of data generated by the legislature, safety, legislation, and business software databases, among other things. Using the block chain and the RSA digital signature mechanism, the proposed system provides dependability and trust in data exchange in communication channels.

Sergey Semushin et al [3] illustrate how a wireless sensor network is an essential component of a system's architecture. Because IoT devices are inherently low-powered and have limited resources, choosing the right encryption technique for WSN communication is critical. In this study, we examine various symmetric block-based cryptographic algorithms to remark on their capabilities, assisting in the selection of the best approach for a given application.With varying block and key lengths, we chose commonly used algorithms such as AES, DES, Triple DES, IDEA. The comparison is based on energy consumption, power consumption, memory utilisation, and throughput.

Saifullah Khan et al [4] Private/confidential data can be stored in a secure manner utilising blockchain technology. Data legitimacy, concealment, authentication, and identification can all be improved by combining encryption methods with a consensus algorithm with associated hash values. Using these two algorithm standards helps to keep data safe and secure while also protecting it from intruders and predators.

A lot of data relating to health records is maintained and transmitted on the cloud, according to Dhananjay Yadav et al [5]. To gain patients' belief, data transmitted between patients and doctors must be secure. Blockchain is a method for securing data in a more advanced manner. The blockchain divides data into bits that are difficult to decrypt, adding an added degree of security. The primary goal of this article is to provide secure and reliable storage of patient data in an effective manner.

Yang Chen et al [6] They offer a method to enhance the cost of a successful 51 percent double-spending attack on Proof-of-Work Blockchain systems in this study. In branch-based selection, the HWD algorithm comes in handy.The attacker has access to compute hash power that is larger than half of the total hash power in this situation.

Shaista Anwar et al [7] have observed As we recognise the importance of managing fraud in the corporate sector, we look back over the past developments in corporate malfeasance in terms of wealth trafficking, forgery, and falsification of financial records by deviating regulations. This primarily draws emerging countries, which have focused their emphasis on various aspects of the country, allowing wicked ideas to set a precedent. Our research is focused on an aspect of accountancy that helps auditors in detecting and preventing corporate fraud early on. should use the Identity Based Cryptography (IBC) framework to create a network node on the ethereum blockchain.

Every cluster in the network will have the same immutable data arrangement, according to Sarada Prasad Gochhayat et al [8]. The Bitcoin network is a collaboration technique to assure synchronisation throughout sites because it is a shared data center. Yugala is a new lightweight, decentralised, encrypted cloud storage system. The Yugala framework ensures data confidentiality, security, and integrity throughout the whole network. The result section displays the architecture's performance, emphasising the high transaction throughput needed in relation to the size of the upload.

Pascal Urien et al [9] the crypt terminal is a new open gadget for safeguarding blockchain wallets, as discussed in this paper. The touch screen, Bluetooth module, detachable smartcard, and processor are all included in this terminal gadget. The encryption standard for producing the secret key during the encryption procedure is included on this detachable smartcard. The terminal's design is bare metal, with Bluetooth connectivity and firmware that can be deleted and uploaded at any moment.

Felipe Zimmerle da N. Costa et al [10] the most popular cryptocurrencies now in use are distributed consensus and blockchain. However, the packages were published to the users with an average delay of 39 minutes. The delay was caused by the block generation and subsequent Voucher action. The publication delay can be considered acceptable

because most packages must be relayed through mirrors, which are likely to have longer delays.

Wolfgang Klas et al [11] the amount of multimedia data, particularly photos, is rapidly expanding. Because the content of images released on the Internet is easily modifiable, they are more likely to be tampered with or changed. When dealing with this issue, blockchain technology offers benefits and challenges Because (a) information in a database is correctly maintained and unchangeable, and (b) inputting info manually onto a network could take a long time, making it operationally and logistically burdensome. As a result, we provide a cryptocurrency solution that considers two important factors: To begin, a blockchain was used to store records regarding creator authorship and trademarks, as well as descriptive data about a photograph, which was then utilised to identify pirated content. Furthermore, rather than storing actual visual content in the ledger, only distinctive informative content regarding all photographs is stored, making the management easier to execute.

Antonina Ferion et al [12] the purpose of this article is to examine the benefits of blockchain technology in terms of improving cyber security. Cyber criminals can attempt to crack large data sets and accounts, which is a well-known factor. Nowadays, security groups organisations fail to guarantee security and data integrity for large data sets, therefore, big businesses are seeking the best-blooming blockchain technology.

Tanishq Harman et al [13] the purpose of an organization's business continuity is to protect its resources from hostile attack. The majority of businesses are aware of security issues and have spent time and money developing a security strategy. The security plan defines the infrastructure, rules, individuals, and activities that must be in place to cope with security vulnerabilities. Nevertheless, computer hackers are on the upswing, and assailants are constantly coming up with new ways to wreak harm. Because it is impossible to avoid assaults, the emphasis seems to be on how to respond to and rebound from strikes quickly. The hacker's sustainable strategy will be supported by recent threats and must be improved on a regular basis.

Sidra Malik et al [14] according to the research conducted for this article, data consistency and visibility are the most critical issues in today's world. The most effective approach to this huge issue is reputation systems. Granularity and automation are both lacking in some systems. The trust chain, as discussed in this paper, is a three-layered architecture that uses consortium blockchain standards to log transactions. For greater performance, reputation scores are also important.

Gang Wang et al [15] most extant architectures are built on centralised storage, which only allows for easy data storage but lacks data consistency and untraceability. By utilising the blockchain's decentralised storage architecture, which allows for storage, access to trustworthy users, data integrity, privacy, and security. The Chain Splitter, for example, has a processing architecture in which the maximum blockchain is housed in the public cloud, although the current relevant frames are saved on the overlay network of the various networks in the proposed design.

Luming Wan et al [16] vehicular ad hoc networks (VANET) Due to the inclusion of mobile devices that may be far from network infrastructure, such new apps may have relatively low network bandwidth. The consequences of queuing delays on blockchain flipping activity, as well as probable infractions of the six affirmations norm for request confirmation, are investigated in this research.

Kun Lv et al [17] over time, these intelligent devices have generated a large amount of real information, but there is still a need for a framework that can effectively integrate and leverage the potential of this immense data. Blockchain allows for the transmission of information at a minimal cost, allowing data from digital sensors to be used to generate commercial importance. The goal of this study is to create an elevated cryptocurrency platform employing distributed network topology, considering aspects of cluster routing, and the PBFT-DPOC consensus algorithm to achieve decentralised autonomous devices that are intelligent.

Sarra Boukria et al [18] the progress of the Internet and network development is accelerated by Software Defined Networking (SDN) technologies. SDN modifies the network's properties in terms of mobility, scalability, and extensibility by logically centralising controllers and enabling a broad communications overview. Furthermore, this growth raises the security risks associated with network interaction. To improve SDN integrity, we present the BCFR solution, which prevents the injection of fake flow rules into SDN data layer devices. We leverage blockchain technology in our solution to ensure controller verification and the consistency of network exchange between the controller and other network nodes.The OpenStack platform and the Onos controller are used in this project. Our proposal's performance is demonstrated by the evaluation findings.

Bih-Hwang Lee et al [19] Hardware and communications security is advancing, and security management is one of them. The Saas service makes use of third-party network infrastructure. Heroku is an example of a public service-oriented architecture (PaaS). It enables a number of programming languages that are utilised in the development of web services. Heroku is a compliance mechanism system for deploying and hosting technological evolution, with embedded communication networks and a sophisticated

ecosystem. Network security, which is managed through encryption methods, is an important concern in cloud computing. The Advanced Encryption Standard (AES) is one way of encrypting data (AES). We use Heroku as a software platform in this article, and then we use AES for information protection.The AES cryptosystem can be employed for data privacy, according to the feasibility assessment. Furthermore, cryptographic protocol delay estimates demonstrate that bigger data sizes result in longer data delay times when encrypting content.

Jagdeep Sidhu et al [20] though Crypto currency (Peer-to-Peer Electronic Cash) solved this dual problem and supplied work with metadata on a shared database, it still has not extended the capabilities of a blockchain above serving as a clear and public transaction platform. The first reference client of Satoshi Nakamoto contained a decentralised trade application, which was eventually removed owing to a lack of funds. We built a set of paid enterprises to support a wide range of business models, along with a fully formed distributed ledger fragmented global market, highly stable transfer, and user's profile identifiers which interconnect a holder to any and all providers switch, in keeping with Nakamoto's vision.

Shubham Desai et al [21], as we all know, the general public is also reliant on cloud storage companies for large data storage. However, external attackers can access the data via this cloud storage provider's service, which operates as an untrusted party. Because cloud storage spends a lot of money on storage space and storage devices, it has a lot of limitations in terms of operational expenses, software quality, and data security. The system is designed such that the data owner can upload the data using a web interface. As a result, the user who has a unique individual secret key to the information that has been uploaded to the cloud storage area in a cryptosystem manner is the only one who has permission.

Sadhu Ram Basnet et al [22] as a Software Defined Network, it provides increased security for the entire virtual network. Using the blockchain standard, file sharing via SDN may be deployed considerably more effectively. As the number of people using networks grows, so does the system's efficiency. The Blockchain Standard over SDN was developed in such a way that it safeguards security and capacity accessibility from unauthorized participants.

JiasiWeng et al [23] we are all familiar with the data plane and control plane architecture of software defined networks. The data plane depicts the programmable perspective of the interfaced network, whereas the control plane offers the controller side of the SDN network. Inside this secure network, the designed technology ensures data security and privacy. In the event of any failures or external incursions, this also improves anonymity, confidentiality, stability, dependability, and tracability.

Meet Shah et al [24] but, this method of storage is not very secure. Blockchain, as an enhanced version of security, is a distributed technique of storing data that improves security in a decentralised manner. The full asset can be used in a secure manner by connecting it to a neighboring node. Due to the fact that blockchain is a secure platform with end-to-end nodes connected in a secure network, data is unchangeable. The user's file is projected to the AES encryption standard using metamask and stored across numerous nodes in the network in the intended system. As a result, the focus of this research is on decentralised secure data storage.

Ryan Henry et al [25] the Ledger is a private, exclusively based on a log of time-stamped data that is cryptographically protected from tampering and revision technology that is currently gaining traction. Since blockchains were first proposed a few years ago, their usage as publicly accessible and verifiable ledgers for online financial transactions has grown in popularity.In the traditional network, only a few methods of privacy addressing are explored, despite the fact that several security-related issues can be seen. ln, which has lately been proposed as a technique to dramatically increase the stability of blockchain technology, has modest potential issues that will likewise necessitate an effective solution. Though other measures to improve anonymity in such route transactions are already appearing, devising scalable techniques for conducting (multihop) money transfers discreetly against a web adversary remains an interesting open topic.

N. Sundareswaran et al [26] the process of authenticating and identifying the identities of both its users, as well as assessing the potential hazards of criminal intentions for the dedicated server, is known as KYC.The traditional physical KYC procedure has a number of flaws, including being low reliable, moment, and expensive. The qualities of Blockchain technology, such as irreversibility, confidentiality, and democratization, make it a better alternative to certain issues. Although existing solutions such as "kyc-chain.com" and "KYC.legal" provide for blockchain-based KYC verification, they also provide a mechanism for papers to be confirmed by a trustworthy network participant.

Tatsuo Mitani et al [27] they explored resource tracing on a permissioned blockchain coupled with a permissionless blockchain in this study. They define and explain the provenance of commodities on the permissioned blockchain as a concealed Markov model. In this paradigm, there is also no fraudulent property rise or decline. Balance is the term for this state. We show that the permissioned blockchain's traceability and balance can be demonstrated with zero

knowledge of the permissionless blockchain while concealing the permissioned blockchain's risk tolerance by encrypting this model with fully homomorphic encryption and applying the zero knowledge proof of unencrypted understanding.They presented a mechanism in which operations and it is possible to verify their existence on the permissioned blockchain, as well as being hidden from the permissionless blockchain. they have received. Authentication is defined as the sequence of transactions. The hidden Markov model has indicated the state of the traceability model. This model's processing has been encrypted with encryption that is entirely homomorphic. Finally, they have demonstrated that the law of balance conservation and traceability Permissioned blockchains can be proven in zero time. Knowledge to the permissionless blockchain while keeping it hidden. Permissioned blockchain's internal asset allocation.

Table -1: Algorithm Comparison

Comparison among algorithms without SDN			
Parameters	Algorithms		
	AES	MD-5	DES
Encryption	Faster	Moderate	Low
Power Consumption	Low	Comparatively low	High
Energy Efficiency	High	Comparatively low	Low
Security	Secure	Less Secure	Prone to Attack in traditional network

Table -2: Performance Comparison

Performance and Security in SDN			
Parameters	AES	MD-5	DES
Node Failure Detection	More secure	Comparatively low	Low
Sink Hole Detection	Detection is Possible	Partially Possible	-
Performance Efficiency	Good	Comparatively good	Moderate

The research done with and without the SDN designed network usage for data transactions in a secure manner by using the most applicable cryptographic algorithms in blockchain technology is shown in tables 1 and 2.

4. CONCLUSIONS

The following findings can be drawn based on a bibliographic evaluation of several research articles and the criteria addressed. The various encryption algorithms of cryptography are prone to data loss, according to many Researchers in the field of distributed ledger technology, as well as the organisation in charge of SDN.

This article provides a detailed examination and comparison of the existing research. Existing solutions have been grouped based on different ways of resolving the congestion issue.

1) Use of SDN network enhancements is the executive summary for congestion problem solutions.

2) Using the most secure and simple algorithms possible

Some studies have proposed a hybrid technique that incorporates all of the above-mentioned solutions. However, a state-of-the-art solution to this problem is required in order to optimise software defined network use and reduce congestion.

REFERENCES

[1] M. Nehe and S. A. Jain, "A Survey on Data Security using Blockchain: Merits, Demerits and Applications," 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), pp.1-5, 2019.

[2] Suma V, “Security And Privacy Mechanism Using Blockchain”. Journal of Ubiquitous Computing and Communication Technologies. 01. pp. 45-54,2019.

[3] I. Makarenko, S. Semushin, S. Suhai, S. M. Ahsan Kazmi, A. Oracevic and R. Hussain, "A Comparative Analysis of Cryptographic Algorithms in the Internet of Things," 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC), pp.1-8, 2020.

[4] S. Khan, A. Jadhav, I. Bharadwaj, M. Rooj and S. Shiravale, "Blockchain and the Identity based Encryption Scheme for High Data Security," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1005-1008, 2020.

[5] D. Yadav, A. Shinde, A. Nair, Y. Patil and S. Kanchan, "Enhancing Data Security in Cloud Using Blockchain," 2020 4th International Conference on Intelligent

Computing and Control Systems (ICICCS), pp. 753-757, 2020.

[6] X. Yang, Y. Chen and X. Chen, "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 261-265, 2019.

[7] S. Anwar, V. K. Shukla, S. S. Rao, B. K. Sharma and P. Sharma, "Framework for Financial Auditing Process Through Blockchain Technology, using Identity Based Cryptography," 2019 Sixth HCT Information Technology Trends (ITT), pp. 099-103, 2019.

[8] S. P. Gochhayat, E. Bandara, S. Shetty and P. Foytik, "Yugala: Blockchain Based Encrypted Cloud Storage for IoT Data," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 483-489, 2019.

[9] P. Urien, "Crypto Terminal: A New Open Device For Securing Blockchain Wallets," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-3, 2020.

[10] F. Z. da N. Costa and R. J. G. B. de Queiroz, "A Blockchain Using Proof-of-Download," 2020 IEEE International Conference on Blockchain (Blockchain), pp. 170-177, 2020.

[11] N. Jnoub and W. Klas, "Detection of Tampered Images Using Blockchain Technology," 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019, pp. 70-73, doi: 10.1109/BLOC.2019.8751300..

[12] A. Farion, O. Dluhopolskyi, S. Banakh, N. Moskaliuk, M. Farion and Y. Ivashuk, "Using blockchain Technology for Boost Cyber Security," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), pp. 452-455, 2019.

[13] T. Harman, P. Mahadevan, K. Mukherjee, P. Chandrashekar, S. Venkiteswaran and S. Mukherjea, "Cyber Resiliency Automation Using Blockchain," 2019 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), pp. 51-54, 2019.

[14] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 184-193, 2019.

[15] G. Wang, Z. Shi, M. Nixon and S. Han, "ChainSplitter: Towards Blockchain-Based Industrial IoT Architecture for Supporting Hierarchical Storage," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 166-175, 2019.

[16] L. Wan, D. Eyers and H. Zhang, "Evaluating the Impact of Network Latency on the Safety of Blockchain Transactions," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 194-201, 2019.

[17] S. Yu, K. Lv, Z. Shao, Y. Guo, J. Zou and B. Zhang, "A High Performance Blockchain Platform for Intelligent Devices," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 260-261, 2018.

[18] S. Boukria, M. Guerroumi and I. Romdhani, "BCFR: Blockchain-based Controller Against False Flow Rule Injection in SDN," 2019 IEEE Symposium on Computers and Communications (ISCC), pp. 1034-1039, 2019.

[19] B. Lee, E. K. Dewi and M. F. Wajdi, "Data security in cloud computing using AES under HEROKU cloud," 2018 27th Wireless and Optical Communication Conference (WOCC), pp. 1-5, 2018.

[20] J. Sidhu, "Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business," 2017 26th International Conference on Computer Communication and Networks (ICCCN), pp. 1-6, 2017.

[21] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1575-1578, 2018.

[22] S. R. Basnet and S. Shakya, "BSS: Blockchain security over software defined network," 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 720-725, 2017.

[23] Jiasi, Weng & Jian, Weng & Jia-Nan, Liu & Zhang, Yue. (2019). Secure Software-Defined Networking Based on Blockchain.

[24] M. Shah, M. Shaikh, V. Mishra and G. Tuscano, "Decentralized Cloud Storage Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 384-389, 2020.

[25] R. Henry, A. Herzberg and A. Kate, "Blockchain Access Privacy: Challenges and Directions," in IEEE Security & Privacy, vol. 16, no. 4, pp. 38-45, July/August 2018.

[26] N. Sundareswaran, S. Sasirekha, I. J. Louis Paul, S. Balakrishnan and G. Swaminathan, "Optimised KYC

Blockchain System," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-6, 2020.

[27] T. Mitani and A. Otsuka, "Traceability in Permissioned Blockchain," 2019 IEEE International Conference on Blockchain (Blockchain), pp. 286-293, 2019.

BIOGRAPHIES

Thyagara jamurthy A

Thyagarajamurthy A is an associate professor at JSS Science & Technology University in Mysore, where he specializes in the Department of Electronics and Communication Engineering. His main area of expertise is Wireless Sensor Networks. Operating systems, mobile computing, and networking are among his specialties. He's worked on a variety of networking-related projects and an automated retail invoice matching system was created for operational efficiency projects.

Anusha M

Anusha M is now pursuing her M.Tech in Network and Internet Engineering at JSS Science & Technology University Mysore in the Department of Electronics and Communication Engineering. Security and networking are two of her main areas of interest. Currently, she is pursuing an internship in the security and digital area. She earned a Bachelor of Engineering degree from GSSS Engineering College in Mysuru. She has experience in Internet of Things, security, embedded systems, and communication projects. She also knows about cryptography and advanced communication.