Block Chain Technology for Data Integrity and Security in Cloud Computing

DR. THANH-CHI PHAN PH.D.
Senior Lecturer, Quang Tri Teacher Training College, Dong Ha, Quảng Trị Province, Vietnam.

Abstract- Data is a vital resource in this day and age; in fact, it directs all corporate choices and the majority of computer-assisted human activities. As a result, threats to the integrity of data are of the utmost importance, as deliberately tampering with data may adversely influence key business choices. This problem is especially prevalent in cloud computing settings, because data owners do not have control over essential data characteristics in those environments, such as the physical storage of data and the control over who may access it. Recent years have seen the rise of blockchain as a fascinating new technology that, among other things, delivers appealing qualities regarding data integrity. The use of the blockchain to combat threats to data integrity may seem like an obvious choice; however, the blockchain's existing limitations of poor throughput, high latency, and weak stability make it difficult to implement any blockchain-based solutions in a practical setting. In this paper, we focus on a case study from the European SUNFISH project, which is concerned with the design of a secure by-design cloud federation platform for the public sector. This allows us to precisely delineate the actual data integrity needs of cloud computing environments as well as the research questions that need to be addressed in order to adopt blockchain-based databases. First, we describe the unanswered questions in research and the challenges that come with trying to find answers to them.

Indexed Terms- Block Chain, Cloud Computing

I. INTRODUCTION

Data is quickly becoming one of the most precious things in today's world. When deciding on any course of action for a company in any of a broad range of fields, including but not limited to health care, education, or public administration, it is essential to bear in mind the significance of the company's overall strategy. The capacity to trust data has thus become vital in light of the fact that computer-assisted human activities are becoming increasingly dependent on data. This is due to the fact that data can now be collected and stored on computers. On the other hand, because data serves such a vital role, it has become an exceedingly tempting target for cyberattacks, the objective of which is to weaken the key CIA traits (Confidentiality, Integrity, and Availability) that data must demonstrate in order to be trusted. These qualities include the capacity to keep information private, maintain its integrity, and make it readily available. These characteristics include the ability to keep data secret while both maintaining its integrity and providing access to it.[1] The level of harm that is caused to a user's ability to trust their data as a result of cyberattacks directed on CIA properties varies according to the properties that are breached. To be more explicit, weakening availability renders it impossible to get data for a specified period of time; despite this, operations are able to be continued as soon as the data are made available once again. However, the original data are still accessible and usable, at least to the extent that is permitted by the harm that has been caused (that is to say, an organisation that is a victim of data leakage may be forced to face economic penalties). A breach of confidentiality results in the disclosure of private data, which cannot be undone. Instead, tampering with the data's integrity is a very destructive assault that will always pave the way for major difficulties with trusting the data.[2,3] This type of attack will always prepare the way for serious problems. Indeed, tampering with data can go unnoticed and maliciously drive processes, either by deleting individual entries (i.e., to delete unwanted traces) or by manipulating particular sections of data (i.e., to impact data consumers' behaviour). This can be accomplished either by deleting individual entries or by modifying certain parts of data. It is possible to achieve this goal by modifying or erasing particular parts of the data. In 2015, Kaspersky Lab uncovered a massive cyberattack that targeted more than one hundred distinct financial institutions located all over the world and stole money from the account balances of customers. The total value of the stolen funds was estimated to be close to one billion dollars1. Once there has been a breach in the data integrity, it is not feasible to access the previous version of the information since it has been lost permanently and cannot be recovered. This is in contrast to the availability and confidentiality of the data. The focus of this work is not on the availability or secrecy of the data; rather, it is on the integrity of the data, given that attacks on data integrity are difficult to detect but incredibly strong. In light of this fact, the focus of this study is not on the availability or confidentiality of the data. Problems with data integrity are made worse with systems that are based on cloud computing since data owners have no control over where their data are held, who can really access them, or in what form they may be accessed.[4] This makes it difficult to ensure that data are accurate and reliable. In spite of this, an increasing number of enterprises, both public and private, are choose to outsource the administration of their data since "it relieves the burden of maintenance cost as well as the overhead of storing data locally."[5] As a consequence of this, addressing the urgent requirement of guaranteeing the data integrity characteristics of cloud computing environments has become an absolutely necessary requirement.[6] It is standard protocol to guarantee that the integrity of data is maintained by employing, on the one hand, cryptographic[7] tools (such as digests and asymmetric keys), and, on the other hand, correct data replication methods. This is done to ensure that the data is not altered in any way. In point of fact, individual bits of data may be signed using the cryptographic tools that are available. [8] This is done so that any attempt at forgery may be rapidly discovered through the use of cryptographic signature validations. This is done for security reasons. In point of fact, it would be necessary to break the secret keys in order for an assault to be effective in order for it to be possible. The attacker would then be able to modify data signatures and circumvent cryptographic integrity checks as a result of this. [9,10] Once the method has been perfected, these assaults are tough to carry out, but once they have been successful, they are practically impossible to detect. [11,12] As a result, making use of the appropriate techniques for data replication is strongly suggested in order to ensure the data's integrity in any circumstance. Because an attacker would have to corrupt all of the replicated data without being found, it is much more difficult to break the integrity of data once it has been copied and spread throughout a set of nodes. This makes it far more difficult to breach the integrity of data. This method of data replication has wide application in real-world contexts, such as in the context of cloud computing environments, which offer an abundance of resources for remote data storage.[13]

- Block chain: Data Integrity, Performance, Stability

The blockchain is a piece of technology that is considered to be relatively cutting edge and has just very recently made its appearance on the market. Its first function was that of a public ledger for the bitcoin digital currency during its early days.[14,15] It is mostly composed of interconnected blocks that are continually linked to one another and chained together, and it also contains records.[16] These copies of the record are stored on each node that makes up a peer-to-peer network.[17] These documents are evidence that the transactions in question were carried out under aliases or pseudonyms. In place of traditional forms of currency, transactions might be conducted using a cryptocurrency such as Bitcoin or any other type of asset.[18] Miners are specialised nodes in the network that are in charge of the decentralised collection of transactions as well as the packaging of these transactions into chain blocks. Miners are responsible for ensuring the integrity of the blockchain.[19,20] Mining is the term used to describe this procedure. For the purpose of reaching a consensus among all miners on newly produced blocks, miners utilise appropriate block generation techniques, which are sometimes referred to as the mining process. Mining is the means through which this is performed. Bitcoin is an example of a permission less block chain, which implies that there are no restrictions put on the ability of a node to participate in the mining process. This is because there is no central authority controlling the blockchain.[21,22] On the other hand, if there is a layer that offers miners authentication and authorization, then the block chain will be seen as being permissioned. Proof of work (PoW) is the basis of the initial mining process, which is still in use today for both the Bitcoin and Ethereum blockchains. PoW is the foundation of the first mining method.[23,24] It is a computationally intensive hashing operation that is regulated according to the so-called blockchain difficulty, which determines the average amount of time needed by miners to finish such a task and create a new block. [25] This difficulty is determined by the number of blocks that have been mined from the beginning of the blockchain. The amount of blocks that have been mined from the beginning of the blockchain serves as the primary determinant of this difficulty. [26] When one miner in a network successfully creates a new block, a copy of that block is broadcast to every other miner in the network.[27] This process is called "broadcasting." They believe that this block is the most recent link to be added to the chain, and they start mining new blocks so that the links can be joined to the chain.[28,29] If we want to keep things simple, we might say that a new block is added to the chain as soon as it is created by a miner. This will help keep things organised. (If numerous miners add a block at the same time, a temporary fork will be created, but it will usually be resolved very quickly because miners are always intended to prioritise the chain that is the longest.) When multiple miners concurrently contribute to a block, a temporary fork is produced in the blockchain. The mining process and the full replication of the blockchain on a large number of nodes both contribute to the Proof-of-Work blockchains' ability to maintain the integrity of their data in ways that are distinct from those of other types of blockchains.[30 These characteristics are a result of the fact that proof-of-work blockchains contain full replications of the block chain on a significant number of different nodes. In point of fact, the contents of a block are checked by every miner before it is added to the chain.[31,32] This happens whenever a new block is added. As a consequence of this, the block is almost non-repudiable and permanent (with the exception of the scenario in which an enemy holds the majority of the miners' hash power and is thus able to fork the chain). If it is assumed that the vast majority of the hash power is controlled by trustworthy miners, then the probability of a fork with a depth of n is given as O(2n).[33,34] Users may now have high confidence that their transactions will be permanently integrated with high certainty if they only wait for a minimal number of nodes to be added (six blocks in the case of Bitcoin).[35] This provides users with high confidence that their transactions will be permanently incorporated. Nevertheless, there is a significant drawback connected with blockchains that are constructed on PoW, and that drawback is performance. This slowness is mostly attributable to the delay that occurs when blocks are broadcast across the network as well as the time-consuming nature of the PoW task.[36] In point of fact, each transaction that is kept on a blockchain has a large confirmation time, which results in a very poor transaction throughput. This is due to the fact that blockchains were not designed to handle high volumes of transactions. This is because there is a very poor throughput of transactions, which is the root cause of the problem.[37,38] The average wait time for a Bitcoin transaction is 10 minutes, despite the fact that the network is capable of processing about 7 new transactions every second. In regards to its potential applications, the dependability of the blockchain is still another essential aspect to take into consideration.[39] There is no academic research that has received widespread recognition that explains either why this has taken place or whether or not it will continue to take place in the future or for how much longer it will continue. One illustration of this is the blockchain technology that underpins Bitcoin, which has, up to this point, performed its duties in a satisfactory manner. The stability features of the PoW-based consensus protocol are still the subject of ongoing discussion, and the currently available "literature does not even provide adequate tools to assess under which economic and social assumptions Bitcoin itself will remain stable."[40] In general, blockchains that are built on Proof-of-Work (PoW) and employ incentive systems that are based on cryptocurrencies are very sensitive to market volatility. As a result, the efficiency of the blockchain in the long run is diminished as a result of this sensitivity.[41]

II. APPLICATION OF THIRD-PARTY AUDITOR

Encryption does not, however, protect the data against harm that is caused by mistakes that are made during the setup process or by software problems. This is due to the fact that encryption only restricts access to the data by outside sourced threats.[42] An audit carried out by an impartial third party is a tried-and-true procedure that may be used in order to provide evidence that the data kept on a distant server has not been modified in any way. In the event that the firm requires it, a third party is able to validate the reliability of the data. A programme known as the Third-Party Auditor (TPA) scheme is open to participation from individuals who are in possession of the skills and expertise required to carry out all auditing processes for ensuring the data's integrity as part of the project. Figure 1 illustrates how the architecture of the TPA scheme may accomplish data integrity and assure the data owner's peace of mind regarding the protection of their data.[43,44] This is shown in the form of a diagram. By having the owner participate in the auditing process, the technique assures that the data for all of the owner's resources that are kept in the cloud are correct by eliminating any potential for human error. According to Zikratov et al. (2017), the drawbacks of this technique for preserving the integrity of data include the requirement for a third party communication channel as well as the susceptibility to man in the middle attacks. The emergence of a third party for the processing of data increases the likelihood that hackers will be able to exploit a wide variety of vulnerabilities in the system. According to Zhu et al. (2019), one of the most important challenges that exist today is the question of how to check and assure the data integrity of massive volumes of data that are kept in the cloud in a secure and efficient manner. The usage of trusted Third-Party Auditors (TPAs) and traditional methods for verifying data integrity, such as encryption techniques to safeguard data stored in the cloud, are being phased out in favour of embracing Blockchain technology.[45] This is being done in order to improve security and save costs. There is a possibility that trust difficulties, which are inherently present in TPAs, might be sidestepped using data integrity mechanisms that are supported by blockchain technology. (Wang and Zhang, 2019).

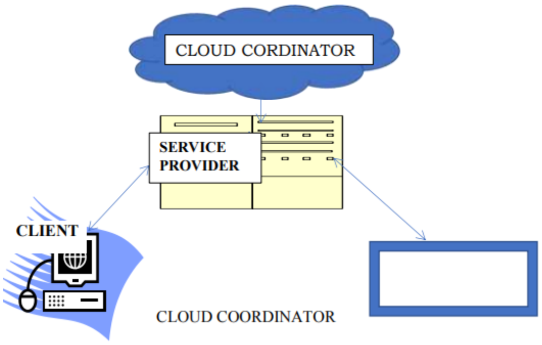

Fig 1. TPA Framework. [46]

III. AN EXAMINATION OF THE SAFETY OF BLOCKCHAIN TECHNOLOGY

In 2008, a distributed ledger technology called the blockchain was initially designed for the Bitcoin platform. This technology has the capability of providing a solution to the problem of trust in a variety of contexts where it may be used. Businesses, such as those in the financial industry, have recently begun researching whether or not blockchain technology may be effective if incorporated into already existing software in order to fulfil the desire for a more transparent and unchangeable audit log.[47] The goal of these investigations is to satisfy the demand for a log that cannot be altered. In the most recent few months, there has been an increase in the amount of attention devoted to the adoption of blockchain applications in a variety of service industries, one of which is the healthcare business. The use of blockchain technology has been proposed as a possible answer to problems relating to patient management and the provision of identities, authorisation to access healthcare data, and the management of participant consent. If emerging cryptographic technologies like blockchain are utilised, there is the possibility that the danger of data tampering will be reduced, and there will be an increase in the level of trust that users have in the data. Blockchain, which is essentially a decentralised database and at the same time functions as the underlying technology of Bitcoin, is one of the most important ideas that are linked with the cryptocurrency Bitcoin. The concept of a blockchain, which may be conceptualised as a chain of data blocks generated by cryptographic operations and is illustrated by Figure 2, is presented here. Each block stores the details of a transaction that was carried out on the Bitcoin network within that block's time period. It is necessary to have this information in order to validate the data in that block and to generate the block that comes next. Blockchain, to put it more briefly, is a chained data structure that sequentially merges data blocks in line with the time sequence.[48] In other words, it is a distributed ledger. In addition to this, blockchain is a distributed ledger that cannot be changed or manufactured since it uses cryptography to record transactions. Using blockchain data structures, blockchain technology is able to verify and store data in a more generic sense.[49] This is made possible through the use of blockchain data structures. It uses encryption to provide safe data transmission and access, distributed node consensus techniques to generate and update data, intelligent contracts made of automated script code to programme and manipulate data, and smart contracts to programme and manipulate data. Additionally, it uses smart contracts to enable secure data transmission and access. Blockchain technology is characterized by a number of defining qualities, including decentralisation, immutability, traceability, collaborative maintenance, openness, and transparency. Consider some of these properties. The characteristics of block chains encourage truthfulness and openness, which are foundational qualities of trustworthy interactions and partnerships. The cornerstone for the numerous application scenarios that are conceivable with the blockchain is the technology's capacity to combat the issue of information asymmetry while simultaneously attaining collaborative trust and concerted action across a variety of issues.[50]

- Applications of Blockchain Technology

Blockchain is a distributed ledger system created in 2008 for Bitcoin. This solution solves trust issues in many use scenarios. Blockchain is both a linked data structure and a distributed ledger that cannot be edited or manufactured due to encryption. To meet the desire for a more transparent and immutable audit record, financial companies have been testing whether blockchain technology can be incorporated into existing software. Blockchain applications in service areas like healthcare have garnered more interest recently. Blockchain technology may be used to handle patient identification, consent, and healthcare data access. Blockchain technology ensures dependability. It uses consensus and encryption to ensure data consistency among nodes. Algorithms compose the distributed ledger. Blockchains link data blocks chronologically.[51] Cryptography protects this distributed ledger against forgery and tampering. Blockchain participants maintain open and transparent node information. Public information is permanent and unchangeable. Cloud computing users may trust the blockchain's open verification and tamper-proof properties. Blockchain technology can boost data security in cloud computing since all findings can be uploaded to the blockchain for authentication and all users can maintain the blockchain. Blockchain data structures verify and store data. IT updates data via distributed node consensus.[52] Smart contracts, which employ automated script code, programme and update data using cryptography. Blockchain technology is decentralised, immutable, traceable, communally maintained, open, and transparent. The blockchain's unique properties defend its honesty and transparency and promote confidence. The blockchain's ability to overcome knowledge asymmetry, generate collaborative trust, and coordinate activity across several areas makes it a versatile tool. created ProvChain, a system that captures provenance data, stores it, verifies it using blockchain technology, and provides a full record when needed. Zhu et al. (2019) created a block chain-based file management solution to handle project document tampering. We proposed a blockchain-based verification technique for P2P cloud storage and used Merkle trees to validate data correctness. Wang, Wang, and He (2019) integrated the PDP scheme with the blockchain to produce the first efficient and secure blockchain-based PDP model. Zhu et al. (2019) suggested utilising blockchain technology to develop a certificate-free system to discourage auditors who take too long.[53] This method can only eliminate procrastinating auditors, not other issues like TPA collaboration. The blockchain is essential in finance, healthcare, and the IoT because to its openness, transparency, and data tracking. Cloud data integrity verification with blockchain technology is still under development. Traditional data integrity verification uses trusted Third-Party Auditors (TPAs) and encryption to protect cloud data. Blockchain-based data integrity schemes can address TPA trust issues. Wang and Zhang (2019) proposed a Blockchain and Bilinear mapping-based Data Integrity Scheme (BB-DIS) for large-scale Internet of Things data to address these issues. BB-DIS prototype that shards Internet of Things data and creates homomorphic verifiable tags (HVTs) for sample verification. BB-DIS performance study, encompassing feasibility, security, dynamicity, and complexity, might achieve data integrity using bilinear mapping in blockchain transactions. An experiment using Hyperledger Fabric showed that the recommended verification approach improved integrity verification for large-scale Internet of Things data without TPAs. Liu et al. (2017) suggest using blockchain to verify data integrity, which might benefit blockchain systems and data storage. Retricoin coins and verifies data integrity using huge file Proofs of Retrievability (POR). POR files replace PoW in this coin.

- An examination of the safeguards already in place to guarantee the accuracy of the data

One of the various ways that are known for assuring the integrity of data is the calculation of checksum values and the comparison of those checksum values with reference values. Other ways for maintaining the integrity of data include those that are based on cryptographic procedures. These methods include key and keyless hashing as well as means of electronic signature . One of the downsides of utilising these methods is that they are unable to ensure their own integrity without also relying on a data recovery mechanism, which is one of the drawbacks of using these methods.[54] Keeping the data in its original form may also be accomplished by the use of duplication methods, redundant coding methods, and RAID technology, which stands for redundant array of independent discs. RAID technology can be implemented through either hardware or software. Utilising a variety of different reservations is one additional strategy that may be utilised to protect the authenticity of the data. When these methods are followed, a large quantity of unnecessary work is produced as a result. trial chain was developed as a blockchain-based platform that could be used to check the data integrity of large scientific research trials. the platform was established by trial chain.[55] This was done in order to improve the visibility of the data amount as well as the analysis that was being carried out. considers the collecting of trustworthy data to be the point at which the successful operation of an analytical system may be said to have begun. This is as a result of the fact that the procedures that are utilised to collect data have a direct bearing on the accuracy of the data. During the course of the study, a private block chain was created by making use of the MultiChain platform.[56] After then, this block chain was merged with a data science platform that had been established inside of a major research institution. Validity checks on the data and documentation of the methods employed in the analysis are an imperative necessity in order to transfer the findings into high-quality therapeutic treatment. Validity checks on the data can help determine whether or not the results can be trusted.

IV. MODELS TO ENSURE DATA INTEGRITY WITH BLOCKCHAIN

When the data is being delivered or stored, it is a highly challenging problem to ensure that the data retains its integrity. Consequently, in order to encrypt data, one needs to use cryptographic methods that take a longer amount of time to complete. The usage of blockchain technology as a means of providing a guarantee for the genuineness of data is examined in this article. Vainshtein and Gudes (2021) presented a novel method of leveraging a PoW-based Blockchain as a way of maintaining data integrity in cloud database management systems. This was done in order to address the problems that emerge when utilising cloud platforms for the storing of data or the hosting of databases. This strategy was established in order to address the challenges that are presented by the use of cloud platforms. [57] The strategy called for establishing some type of link between the cloud platform and a Blockchain system that operated on the proof-of-work principle. This method makes use of a Distributed Hash Table in conjunction with lightweight software agents in order to monitor any changes that are made to cloud database storage nodes. The goal of this method is to maintain track of any changes that are made.[58] This is important since there is no straightforward method for a customer to verify the accuracy of the data that is kept in a cloud database. As a result, this is required. The agents, when they interact with one another, will broadcast the data update activities into the Blockchain network in the form of Blockchain log/audit transactions until such time as they are cryptographically and permanently protected by it.[59] The method that has been described enables the Cloud Provider to manage the metadata in order to rapidly detect deliberate or accidental corruptions of transactions and recover transactions in the event that any data corruption incident takes place. This solution was offered by the authors of the aforementioned research paper. The question of how to verify and assure the data integrity of enormous volumes of data that are kept in the cloud in a way that is both safe and efficient is one of the most serious concerns of our day. The previous method of data integrity certification, which depended on trusted Third-Party Auditors (TPAs) and encryption measures to secure data stored in the cloud, is being phased out in favour of blockchain technology as the new standard. Because of its superior level of safety, blockchain technology is gradually displacing the more traditional technique of verifying the integrity of data.[60] There is a possibility that trust difficulties, which are inherently present in TPAs, might be sidestepped using data integrity mechanisms that are supported by blockchain technology. A Blockchain and Bilinear mapping-based Data Integrity Scheme, abbreviated as BB-DIS, was presented by Wang and Zhang (2019) for large-scale Internet of Things data in order to tackle the issues that were produced by TPAs. In order to generate homomorphic verifiable tags (HVTs), the data from the Internet of Things were sharded first.

This step was done for the purpose of sample verification. The features of bilinear mapping were adhered to in order to guarantee the authenticity of the data, and this was accomplished through the utilisation of blockchain transactions.[61

CONCLUSION

The data storage on a blockchain is completely decentralised, which indicates that all of the nodes in the network collaborate to keep the data up to date, while some of the nodes in the network just store backup copies of the data. On the other hand, traditional distributed databases gather all of their information into a single central server node and store it there. If the data stored in a single node in the blockchain is damaged, removed, or altered in any other way, this will not have any effect on the data that is recorded in the blockchain. Only if more than 51% of the nodes engaged in an attack work together to change the data, which is stored on the blockchain, is it possible for the data to be changed. As a consequence of this, the data that is saved on the blockchain may be considered immutable so that it may be saved in a secure manner. Data is protected from bad actors by the blockchain system, which also defends against the risk of fraudulent behaviour and reduces the probability that data would be stolen or compromised in another way . In conclusion, adopting blockchain technology as the third-party authentication platform may safeguard user privacy while also assuring the availability of data, enhanced security, and greater efficiency. These benefits may be achieved through a combination of these factors. Viewing digital information, securely sharing and keeping it, and doing so all become considerably less complicated when blockchain technology is utilised. In addition, it protects each transaction by encrypting the data using cryptographic methods. It is possible that when firms do this, they will take the existing high levels of security and openness that they have to a whole new level.

REFERENCES

[1] Haug, C. J. (2015). Peer-review fraud—hacking the scientific publication process. New England Journal of Medicine, 373(25), 2393-95. http://doi/ 10.1056/NEJMp1512330

[2] Rosak-Szyrocka, J., Żywiołek, J., & Shahbaz, M. (Eds.). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.). Routledge. https://doi.org/10.4324/9781003404682

[3] Dr. Shashi Kant Gupta, Hayath T M., Lack of it Infrastructure for ICT Based Education as an Emerging Issue in Online Education, TTAICTE. 2022 July; 1(3): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.03. A004

[4] Hayath T M., Dr. Shashi Kant Gupta, Pedagogical Principles in Learning and Its Impact on Enhancing Motivation of Students, TTAICTE. 2022 October; 1(2): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.04. A004

[5] Shaily Malik, Dr. Shashi Kant Gupta, “The Importance of Text Mining for Services Management”, TTIDMKD. 2022 November; 2(4): 28-33. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04. A006

[6] Dr. Shashi Kant Gupta, Shaily Malik, “Application of Predictive Analytics in Agriculture”, TTIDMKD. 2022 November; 2(4): 1-5. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04. A001

[7] Dr. Shashi Kant Gupta, Budi Artono, “Bioengineering in the Development of Artificial Hips, Knees, and other joints. Ultrasound, MRI, and other Medical Imaging Techniques”, TTIRAS. 2022 June; 2(2): 10–15. Published online 2022 June doi.org/10.36647/TTIRAS/02.02. A002

[8] Dr. Shashi Kant Gupta, Dr. A. S. A. Ferdous Alam, “Concept of E Business Standardization and its Overall Process” TJAEE 2022 August; 1(3): 1–8. Published online 2022 August

[9] A. Kishore Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "An Enhanced Genetic Algorithm for Solving Trajectory Planning of Autonomous Robots," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099994

[10] S. K. Gupta, V. S. Kumar, A. Khang, B. Hazela, N. T and B. Haralayya, "Detection of Lung Tumor using an efficient Quadratic Discriminant Analysis Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC),

Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111903.

[11] S. K. Gupta, A. Alemran, P. Singh, A. Khang, C. K. Dixit and B. Haralayya, "Image Segmentation on Gabor Filtered images using Projective Transformation," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111885.

[12] S. K. Gupta, S. Saxena, A. Khang, B. Hazela, C. K. Dixit and B. Haralayya, "Detection of Number Plate in Vehicles using Deep Learning based Image Labeler Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111862.

[13] S. K. Gupta, W. Ahmad, D. A. Karras, A. Khang, C. K. Dixit and B. Haralayya, "Solving Roulette Wheel Selection Method using Swarm Intelligence for Trajectory Planning of Intelligent Systems," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, doi: 10.1109/ICRTEC56977.2023.10111861.

[14] Shashi Kant Gupta, Olena Hrybiuk, NL Sowjanya Cherukupalli, Arvind Kumar Shukla (2023). Big Data Analytics Tools, Challenges and Its Applications (1st Ed.), CRC Press. ISBN 9781032451114

[15] Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C. (2017). A DistributedLedger Consortium Model for Collaborative Innovation. IEEE Computer. 50 (9), 29-37. http://doi: 10.1109/MC.2017.3571057.

[16] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017). Towards Data Assurance and Resilience in IoT Using Blockchain. IEEE Military Communications Conference, 261-266. doi: 10.1109/MILCOM.2017.8170858.

[17] Omoyiola, B. O. (2018a). Overview of biometric and facial recognition techniques. IOSR Journal of Computer Engineering (IOSRJCE). 20(4), 1-5.doi: 10.9790/0661-2004010105.

[18] Omoyiola, B. O. (2018b). The legality of ethical hacking. IOSR Journal of Computer Engineering (IOSR-JCE). 20(1), 61-63.doi:10.9790/0661-2001016163.

[19] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. Proceedings of the 16th ACM conference on Computer and communications security. 199–212. https://doi.org/10.1145/1653662.1653687

[20] Akeson, J. K. (1989). Assuring system data integrity-An overview. 1989 IEEE Global Telecommunications Conference and Exhibition 'Communications Technology for the 1990s and Beyond', (1), 217-22. http://doi.org/ 10.1109/GLOCOM.1989.63970.

[21] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71. https://j2-capital.com/wpcontent/uploads/2017/11/AIR-2016-Blockchain.pdf

[22] Davidson, S., De Filippi, P., & Potts, J. (2016). Economics of blockchain, SSRN. http://dx.doi.org/10.2139/ssrn.2744751

[23] Dorri, A., Kanhere, S.S, Jurdak, R., Gauravaram, P (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity, Journal of Parallel and Distributed Computing, 134 (2019). 180-197, https://doi.org/10.1016/j.jpdc.2019.08.005.

[24] Gao, W., Chen, L., Hu, Y., Newton, C.J.P, Wang, B., & Chen, J. (2019). Lattice-based deniable ring signatures. International Journal of Information Security, 18, 355–370 (2019). https://doi.org/10.1007/s10207-018-0417-1.

[25] Yue, D., Li, R., Zhang, Y., Tian, W., & Peng, U. (2018). Blockchain-based data integrity verification in P2P cloud storage. IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 561-568. http://doi.org/ 10.1109/PADSW.2018.8644863.

[26] Vainshtein, Y., & Gudes, E. (2021). Use of Blockchain for Ensuring Data Integrity in Cloud Databases. In: Dolev S., Margalit O., Pinkas B., Schwarzmann A. (eds) Cyber Security Cryptography and Machine Learning. Lecture Notes in Computer Science, 12716. https://doi.org/10.1007/978-3-030-78086-9_25

[27] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik. Scalable and efficient provable data possession. In Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, pages 1–10, 2008.

[28] G. Chairscott, L. Michael, P. Chairpeterson, and Larry. Proceedings of the nineteenth acm symposium on operating systems principles. 2003.

[29] B. Chen and R. Curtmola. Robust dynamic remote data checking for public clouds. In Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), pages 1043–1045. ACM, 2012.

[30] R. Curtmola, O. Khan, R. Burns, and G. Ateniese. Mr-pdp: Multiplereplica provable data possession. In The 28th International Conference on Distributed Computing Systems (ICDCS2008), pages 411–420. IEEE, 2008.

[31] Y. Deswarte, J.-J. Quisquater, and A. Sa¨ıdane. Remote integrity checking. In Integrity and Internal Control in Information Systems VI, pages 1–11. Springer, 2004.

[32] H. He, R. Li, X. Dong, and Z. Zhang. Secure, efficient and fine-grained data access control mechanism for p2p storage cloud. IEEE Transactions on Cloud Computing, 2(4):471–484, 2014.

[33] W. U. Ji-Yi, F. U. Jian-Qing, L. D. Ping, and Q. Xie. Study on the p2p cloud storage system. Acta Electronica Sinica, 35(5):1100–1107, 2011.

[34] A. Juels and B. S. Kaliski Jr. Pors: Proofs of retrievability for large files. In Proceedings of the 14th ACM Conference on Computer and Communications Security, pages 584–597. ACM, 2007.

[35] Wang, H., Wang, Q., & He, D. (2019). Blockchain-Based Private Provable Data Possession, IEEE Transactions on Dependable and Secure Computing, 18(5), 2379-2389. http://doi.org/10.1109/TDSC.2019.2949809.

[36] Navaneetha Krishnan Rajagopal, Mankeshva Saini, Rosario Huerta-Soto, Rosa Vílchez-Vásquez, J. N. V. R. Swarup Kumar, Shashi Kant Gupta, Sasikumar Perumal, "Human Resource Demand Prediction and Configuration Model Based on Grey Wolf Optimization and Recurrent Neural Network", Computational Intelligence and Neuroscience, vol. 2022, Article ID 5613407, 11 pages, 2022. https://doi.org/10.1155/2022/5613407

[37] Navaneetha Krishnan Rajagopal, Naila Iqbal Qureshi, S. Durga, Edwin Hernan Ramirez Asis, Rosario Mercedes Huerta Soto, Shashi Kant Gupta, S. Deepak, "Future of Business Culture: An Artificial Intelligence-Driven Digital Framework for Organization Decision-Making Process", Complexity, vol. 2022, Article ID 7796507, 14 pages, 2022. https://doi.org/10.1155/2022/7796507

[38] Eshrag Refaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[39] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[40] Bramah Hazela et al 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[41] Ashish Kumar Pandey et al 2022 ECS Trans. 107 2681 https://doi.org/10.1149/10701.2681ecst

[42] G. S. Jayesh et al 2022 ECS Trans. 107 2715 https://doi.org/10.1149/10701.2715ecst

[43] Shashi Kant Gupta et al 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[44] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[45] S. K. Gupta, B. Pattnaik, V. Agrawal, R. S. K. Boddu, A. Srivastava and B. Hazela, "Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936404.

[46] Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. *Infrastructures***2023**, *8*, 22. https://doi.org/10.3390/infrastructures8020022

[47] V. S. Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Natural Language Processing using Graph Neural Network for Text Classification," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060655.

[48] M. Sakthivel, S. Kant Gupta, D. A. Karras, A. Khang, C. Kumar Dixit and B. Haralayya, "Solving Vehicle Routing Problem for Intelligent Systems using Delaunay Triangulation," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060807.

[49] S. Tahilyani, S. Saxena, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Deployment of Autonomous Vehicles in Agricultural and using Voronoi Partitioning," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060773.

[50] V. S. Kumar, A. Alemran, S. K. Gupta, B. Hazela, C. K. Dixit and B. Haralayya, "Extraction of SIFT Features for Identifying Disaster Hit areas using Machine Learning Techniques," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060037.

[51] V. S. Kumar, M. Sakthivel, D. A. Karras, S. Kant Gupta, S. M. Parambil Gangadharan and B. Haralayya, "Drone Surveillance in Flood Affected Areas using Firefly Algorithm," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060857.

[52] Parin Somani, Sunil Kumar Vohra, Subrata Chowdhury, Shashi Kant Gupta. "Implementation of a Blockchain-based Smart Shopping System for Automated Bill Generation Using Smart Carts with Cryptographic Algorithms." CRC Press, 2022. https://doi.org/10.1201/9781003269281-11.

[53] Shivlal Mewada, Dhruva Sreenivasa Chakravarthi, S. J. Sultanuddin, Shashi Kant Gupta. "Design and Implementation of a Smart Healthcare System Using Blockchain Technology with A Dragonfly Optimization-based Blowfish Encryption Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003269281-10.

[54] Ahmed Muayad Younus, Mohanad S.S. Abumandil, Veer P. Gangwar, Shashi Kant Gupta. " AI-Based Smart Education System for a Smart City Using an Improved Self-Adaptive Leap-Frogging Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003252542-14.

[55] Shobhna Jeet, Shashi Kant Gupta, Olena Hrybiuk, Nupur Soni (2023). Detection of Cyber Attacks in IoT-based Smart Cities using Integrated Chain Based Multi-Class Support Vector Machine (1st Ed.), CRC Press. ISBN 9781032451114

[56] Parin Somani, Shashi Kant Gupta, Chandra Kumar Dixit, Anchal Pathak (2023). AI-based Competency Model and Design in the Workforce Development System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[57] Shashi Kant Gupta, Alex Khang, Parin Somani, Chandra Kumar Dixit, Anchal Pathak (2023). Data Mining Processes and Decision-Making Models in Personnel Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[58] Alex Khang, Shashi Kant Gupta, Chandra Kumar Dixit, Parin Somani (2023). Data-driven Application of Human Capital Management Databases, Big Data, and Data

Mining (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[59] Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta, Anchal Pathak (2023). Data-centric Predictive Modelling of Turnover Rate and New Hire in Workforce Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[60] Anchal Pathak, Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta (2023). Prediction of Employee's Performance Using Machine Learning (ML) Techniques (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[61] Worakamol Wisetsri, Varinder Kumar, Shashi Kant Gupta, "Managerial Autonomy and Relationship Influence on Service Quality and Human Resource Performance", Turkish Journal of Physiotherapy and Rehabilitation, Vol. 32, pp2, 2021.