Mammu'an Titus Alams , 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Augmenting Data Integrity with Blockchain Technology

Mammu'an Titus Alams, Godwin A. Thomas, Stephen Mallo Jr, David E. Ogwuche , and Betty T. Dimka

Department of Computer Science University of Jos, Jos, Plateau State, Nigeria

Abstract - In many critical sectors such as finance, healthcare, and supply-chain management, data security is important because data breaches or errors can cause severe damage. Blockchain technology promises that data cannot be altered or deleted once recorded making it free from forgery or unauthorized modifications. This is in contrast to traditional databases that allow data to be changed or removed without any trace which could result in potentially integrity problems. Unlike conventional centralized databases which are typically prone to manipulation, blockchain uses cryptographic algorithms where each block in the blockchain is directly linked with cryptographic algorithms making it impossible for anyone to change the records without being detected thereby ensuring that stored information is highly reliable. While there are obstacles such as scalability as well as energy consumption, blockchain has features unique that position it as a transformative technology to secure and ensure the integrity of stored records. Especially in decentralized, distributed, and untrusted environments, blockchain technologies present qualifying characteristics that allow it to uphold the authenticity and integrity of data in different applications. This paper explores the prospects of integrating Blockchain into database technologies to enhance their ability to maintain data integrity and validity. The research employs a comparative analysis of the traditional databases and blockchain approaches to data integrity to output the findings in terms of their strengths and limitations.

Keywords - Database, blockchain, data integrity, decentralization.

I. INTRODUCTION

The Idea of blockchain was first introduced in 2008 with the digital cryptocurrency called bitcoin, which runs on a blockchain [1]. Blockchain is a technology initiated for record keeping, basically associated with a currency called tokens. Blockchain keeps records of financial transactions in a digital ledger that decentralizes the records [2]. This pool of records can be distributed between users and kept in a chain of transactions rather than leaving all records with just an individual (agency) [2]. Although Blockchain is seen as a medium for digital currency, there are other blockchain technological applications such as smart contracts, consensus, unique governance, and so on [2; 3].

Data stored on the blockchain are in blocks connected conceptually by a chain, the blocks are chained cryptographically and digitally signed [3]. The primary feature of blockchain is adding new blocks to an existing end of blocks this means that new transactions carried out can only be added to the end of the existing chain of blocks but not updating or deleting any old record as done on the traditional database management system such as MySql, Oracle database and so on [2;4]. Blockchain can maintain the exact and real data transaction with clear non-repudiation of stored data as referencing can be done to any transaction carried out on a block as no chain can be altered since completeness, accuracy, and consistency of data are maintained [5].

The set of growing lists of blocks on a blockchain contains data headers that uniquely identify a chain

of blocks, this block header contains the metadata of each block [2; 6]. Block metadata basically has details of block version, creation time, transaction time, previous block hash, and recent block added to the chain [7]. To alter a block is to alter or update a certain transaction is to alter the block header metadata but each block contains the pointer to the previous block this means to alter the whole block of chains because if a block is altered it breaks the chain [7]. Figure 1 shows how transactions are carried out from one block to another and the current transactions are added to the existing chain of blocks without altering any data of the previous blocks.

Figure 1. How transactions are stored on blockchain [7]

Blockchain is controlled by a peer-to-peer network and is based on the concept of decentralization of all transaction chains of blocks to nodes identified by Public Key (PK) cryptography [6]. The shared transaction between the entire nodes uses the Public Key encrypted format. The PK is used for verification and validation of trust between nodes before communicating with other nodes or decentralizing transactions [6].

The rest of the section talks about data storage in general, what integrity is all about in general terms, the architecture of blockchain and how data is stored on the blockchain explaining the blocks in detail, the integrity of data stored on blockchain due to its nature of architecture and why data from blockchain or transactions on blockchain should be trusted over other traditional means of storage.

II. MATERIALS AND METHODS

This research paper employs a comparative analysis method to assess and evaluate data integrity between traditional databases and blockchain technology. The study involved a sound literature review and logical reasoning to conclude the relative merits of both systems. It began with a literature review to gather insights from academic journals, technical reports, and industry whitepapers, focusing on data storage mechanisms, security features, and integrity maintenance. Key features of traditional databases, such as unique key IDs, CRUD operations, and various integrity constraints, are identified and compared with blockchain's unique attributes, which include decentralization, immutability, consensus mechanisms, and digital signatures.

The comparative analysis logically assessed how each technology's features contribute to maintaining data integrity with the findings highlighting that while traditional databases have effective mechanisms for data integrity, they are susceptible to challenges like data redundancy and unauthorized access. In contrast, blockchain technology, with its decentralized and immutable nature, provides superior data integrity, especially for applications requiring high security and tamper-proof data storage. This methodical comparison stresses the blockchain's potential as a robust model for ensuring data integrity, particularly in situations where preventing forgery, fraud, and third-party interference is crucial.

III. DATA IN STORAGE

Since their inception in the 1960s, databases have evolved, with hierarchical and network databases, through the 1980s with object-oriented databases, which led to more flexible options of databases like SQL, NoSQL, and Cloud databases [8]. Data needs a well-organized and secure storage base for record retrieval at any point. Storage-based, referred to as a database, is a well-defined set or collection of data, organized in such a way that it can be easily retrieved and updated, that is, proper keeping of some sort. Database storage refers to the collective technique, methods, and technologies used for the arrangement of data in whatever model chosen, with the most prevalent being the relational model.

In this model, data are stored in tables, which are kept on the hard disk of the database server. These tables are often divided into columns and rows, whereby the columns specify the information category and data type while the row contains the actual data. The key feature of this model is its ease of use.

The data in storage, depending on how and where is recorded can be typically stored in one of the forms below:

- Ordered/Unordered Flat Files: Here data is stored in plain text format and contains one record per line.

- Heap Files: This represents a tree-based data structure, where there is always a root node, which is always bigger or at least equal to its child node. The child nodes of the root's child nodes are again of equal or less value compared with their parent and so on.
- B+ tree: This is the most widely used data structure, which is an improved version of the B-tree structure. It is a kind of tree that can easily be indexed, searched, and edited.
- ISAM: Originally developed by IBM for fast indexing and retrieval purposes. It contains a special set of indexes, which index all records and allow for faster search times, since the search will go through the indexes and not the actual records [9].
- The traditional database architecture consists of a finite four important sections that define the flow of data from the user to the storage end (readable data from the user view to the complex view) [9].

IV. DATA INTEGRITY

The word integrity is often associated with all parts of information security. Data integrity comes with data sharing, either sending or retrieving but ensuring that data is exact and not altered in transit at all times. Data exchanged by authorized entities must be free of content modification (insertion, reordering, deletion, and so on) by an unauthorized entity [10]. Integrity is important to prevent an intruder from concealing his or her activities on data in transit [10]. Tempering with data is a common practice that is done intentionally or mistakenly in rare cases and sometimes difficult to notice if an integrity check is not carried out. Data cannot be understood if there is no metadata that gives additional information about it [11]. Information that well describes data in its form, and assists in managing the data is referred to as the metadata of that data [11]. The completeness and consistency of data are beyond maintaining just the data and ensuring the metadata is not altered so that integrity is completely maintained.

Data integrity has a broad definition according to different professions, which clearly defines how data should be maintained throughout its life cycle to avoid any data corruption, modification, or omission in any system [9]. Some of the basic definitions by different professions are as follows:

- To a security officer data integrity is the assurance that legitimate and authorized users can only access required information.
- To a database administrator data integrity is associated with data stored and entered into a database that must be original, valid, and persistent with other attributes of data integrity such as entity integrity, domain integrity, and referential integrity must be maintained [12].
- To a data architect, data integrity is ensuring attributes that uniquely identify an entity instance should be unique and must contain a value to avoid repetition of the data set (11; 12).
- This means that trust is implicitly the essential part of data integrity but this depends on how, and where data is stored and what is the source of the data.

V. DATA INTEGRITY IN TRADITIONAL DATABASE

It is a fact that technology is changing society and changing how almost everything is done. At the center of all this "Data" is the most valuable asset,

where it comes from, how it is managed and used. Reliable access to data is a prerequisite for most systems and several factors could cause unexpected or unauthorized modifications to this data [5;13]. Sivathanu, Wright, and Zadok [14] stated that the main causes of integrity in data are hardware or software malfunctions, malicious activities, or inadvertent user errors. When a minor integrity violation is not properly checked in good time, it could cause further loss of data. For example, a bit-flip while reading a file system inode bitmap could cause the file system to overwrite an important file.
Malicious intrusion can also cause integrity violations. A big chunk of these attacks are caused by malicious modifications of disk data. When an attacker has gained administrator privileges that could be a potential threat to the system. Therefore, prompt detection of integrity violations is vital for the reliability and safety of the stored data [13].

Hackers are extremely sophisticated and will continue to get more sophisticated. Not only do they have the potential to penetrate firewalls and other barriers, but also, they have also learned to cover their tracks after they are done.
Jensen [15] stated guidelines for maintaining the integrity of stored data include:

- Data must be unchanged and secure from all forms of modifications.
- Data must be retained throughout the data lifecycle.

- Data records must be complete and contain all activities about it.
- Stored data must be accompanied by all metadata, as well as appropriate validation data.
- Data must be stored in a way that prevents deterioration.

VI. HOW IS DATA STORED ON BLOCKCHAIN

Decentralized peer-to-peer systematic blockchain data transaction and immutability storage capability associated with other protocols on blockchain networks is a secure new data structure that holds complete trusted records of data integrity of blockchain data [16]. Linear sequence structure of blocks chained together with cryptographic hashes on current blocks added to the chain are referenced to the previous chain, i.e. each chain has a corresponding hash with its successor chain altogether.

Types of blockchain
Although it depends on what a blockchain will be used for, a blockchain is considered to be deployed in two major ways which are associated with its method of interaction or consideration of its functions and uses. A blockchain can be designed and deployed as:

- Permission: this is not a restricted blockchain, all nodes on this blockchain directly send or read transactions carried out by all nodes created on the blockchain [17].
- Permission-less: this is a restricted blockchain, on this blockchain only nodes that are added can write and read transactions on all nodes meaning is not open [17].

Block in a blockchain
Blockchain by design defines a specific type of database: it is a write-once read-only type of data storage. What that means is the design is to be only ever created, and not edited or deleted. A block in a blockchain holds complete information about each transaction and records. The block in a blockchain is generally divided into two sections, which are the block header and block body:

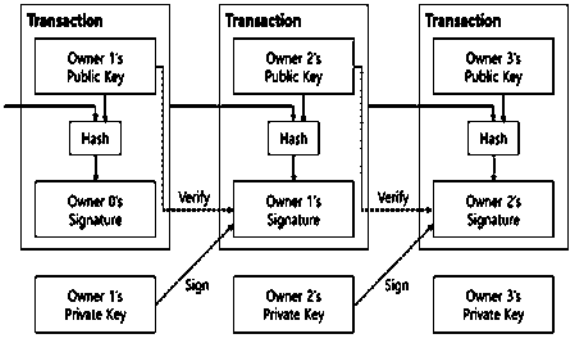
- Block header: holds key information about the transaction and maintains consistency of the block, the block header keeps track of the block version, the hash value of the predecessor block, the timestamp of creation and transaction, and the hash value of the transaction between blocks [5]
- Block body: holds the current transaction carried out on each block and serves as a transaction counter tracker that counts the number of transactions carried out within a successful blockchain cycle [5].

How blockchain works

Blockchain depends on certain variables that aid its functionality to successfully share information and asset exchange without any central authority that controls information sharing [18;19;20;21]. Network participants, consensus protocol controls, cryptography hashes, and digital signatures provide confidentiality, authentication, accountability, and trust between peers. Blockchain can be a secure decentralized data structure for ;

- Confidentiality with Encryption
- Authentication via Digital Signature
- Web of Trust via identity validation from peers

Bitcoin for instance, which is a digital currency that runs on public blockchain has a verifying block for each transaction carried out on the blockchain. Each of the blocks consists of a header and a body. As shown in figure 2. The header consists of the hash values (previous and current) and none of the previous transactions and awaits the creation of the same hash value for the next transaction [18;20]. Verification of each transaction is carried out with public key-based values and hash functions that aid security during the decryption process [18,19]. To determine that nothing is altered the hash value is used for that and the nonce to create the next block, this means that all values from the root hash must be changed before all blocks could be altered [18,19].



DATA INTEGRITY

The nature of data is kept in check using a relational model, which defines the operational consistency between fields in tables, and the source data values to be saved in a particular field with the same attribute. The overall structures of data values must follow a particular domain definition and the defined domain must have permissible values of attributes where those attributes and the data values from a source must belong to its defined domain, which holds one or more values of similar attributes [22]. The nature of data input must exactly be maintained from its source to its storage destination as the front-end input fields and the backend have the same attributes.

Key Constraints: A key is generally used as a unique identifier, which uniquely identifies relationships between relations of one or two attributes. This key ties attributes to a particular relation to avoid duplication of such attributes. Data redundancy is duplication of data and too much duplication of data affects its integrity, updates made to one entry must be updated to all entries associated with that data. Data anomalies will occur if one update is not done and this will affect the data integrity. Key constraints help in the proper normalization of data to reduce redundancy [8; 22].

The regular data future that constitutes the nature of data and key constraints are carried out using the functions:

- Create: adding new records to the database,
- Read: retrieving or reading already existing records,
- Update: altering existing records created and
- Delete: removing existing records saved or created.

Blockchain and the regular way of data storage (database) have a lot of similarities, but trust and robustness are distinct features of the blockchain [23;24] Trust and robustness of the blockchain were explained in different sections above. Aside from the block itself, another key concept of a blockchain is the smart contract, which is a piece of computer code that runs on each node of a blockchain this code shares transactions without a central administrator, meaning all nodes act independently without centralizing trust on a particular node or superior node [2; 23; 25]. Blocks are defined and consist of certain structures such as block version, parent block hash, Merkle tree root, timestamp, nBits, and nonce aside, the current block having the previous hash of its preceding block.

Blockchain integrity is maintained by its immutability capability. This immutability consists of previous hash codes shared between blocks, which maintain transaction integrity stored in chain format. A digital signature is another key component that maintains integrity whereby each user on the network owns a private key and a public key used for signing and verification of transactions [5; 19; 23].

Although the regular (traditional database) and blockchain have common characteristics and some exceptional characteristics that distinct the two methods of storage for example in the case of blockchain digital signatures reside on the block, between end users and the blockchain network but in the case of regular data storage digital signature comes into place during transaction between the application and the database. Table 1 below shows common and distinct features between each method.

Property	***Blockchain***	***Traditional Data Integrity***
Centralization	No	Yes
Previous Hash	Yes	No
Decentralization	Yes	Yes
Consensus	Yes	No
Immutability	Yes	No
Unique keys	No	Yes
Chain data	Yes	No

VIII. SUMMARY OF FINDINGS

The traditional method of storage is known for its unique key ID that controls the movement of data (writing, editing, deleting, and retrieving) between different endpoints however, blockchain has its unique feature of the previous hash and consensus algorithm that helps in finality when data is being written to the blockchain. Sections II, V, and VI above have shown how data are stored between the two storage and presented the distinct features between the two methods of storage, but although not in all instances both storage can be used in the case of trying to eliminate forgery, fraud, storage for large data and elimination of third party as in the case of blockchain in which it can maintain the integrity of data in such systems and in the case of a normal storage or repository system the normal database system could be used for large storage purpose and systems alike.

While databases can use salting, encryption, and other methods to maintain data integrity during storage and transit, blockchain technology offers a more robust approach due to its inherent features. These include consensus mechanisms, immutability, decentralization, and transparency, which collectively provide a higher guarantee of data integrity than traditional database systems.

This shows that blockchain could serve as a model for data integrity, because it can hold sensitive tempered proof data mostly and maintain data originality, although the regular storage could hold sensitive data but since its data are not chained, data could be altered and tracks could be erased.

IX. Discussion

Data's reliability and trustworthiness in traditional database systems depend to a large extent on its integrity. Data integrity is somewhat maintained by the relational model that enforces proper coherency across fields in tables. In the relational model, data is organized into tables that are composed of rows and columns. Each column specifies an information category with a specific data type, while each row contains the actual data.

In conventional databases, there exist several notable constraints and regulations that have been put in place as preventative measures for maintaining data integrity. They include entity integrity, domain integrity, referential constraints, and key constraints. Entity Integrity ensures that every record within a table possesses a unique identifier known as a primary key attribute. Similarly, domain integrity guarantees that values stored under every attribute conform to certain predetermined limits or sets of values. Moreover, referential integrity creates links between these tables ensuring foreign keys match primary keys in related ones preventing any inconsistencies or orphans occurring within data.

Additionally, such regular activities like the creation of new records, reading attributes' contents, updating existing records, and deleting them from within the storage structure i.e., CRUD operations are frequently performed on databases for effective administration purposes. Once again, assuming they have been performed correctly; these operations maintain the front-end input fields' consistency with the backend storage, ensuring data accuracy and reliability.

However, even the most effective mechanisms used in ordinary databases are still vulnerable to some challenges. Inaccuracies can occur when data is duplicated across tables (data redundancy) and updates are not successfully propagated. Maintaining consistency of data throughout distributed systems or during concurrent transactions may also be difficult and lead to anomalies. Also, traditional databases are prone to unauthorized access and data tampering which makes data integrity a constant worry.

Blockchain technology represents a revolution in terms of data integrity; it has come up with new solutions for the problems faced by traditional database systems. Nonetheless, blockchain differs from ordinary database systems through its distinctive features that make it better in terms of data integrity.

Its decentralization is one of the core attributes of blockchain. While conventional databases store information under the control of a central authority, blockchain uses a peer-to-peer network instead. Data duplication takes place across numerous nodes such that no single entity controls all the information. This characteristic aids in increasing transparency as well as making recovery hard should there be any malicious attempts on the system.

As regards blockchain, another crucial characteristic is immutability which has a direct effect on data integrity. When the data has been written into a block, it becomes immutable or unalterable and cannot be corrected or deleted. The blocks are linked together by using cryptographic hashing whereby any change to the information contained in one block would result in changing the hash of that block as well as all subsequent blocks in the chain. This property ensures that data remains untampered throughout its lifecycle.

In addition, consensus mechanisms play a critical role in maintaining data integrity within blockchain networks. Through utilizing consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS), blockchain requires all participants within the network to agree upon transaction validity before their incorporation into this technology. As such, there is no central authority required hence reducing chances of tampering with information.

Moreover, blockchain's dependence on digital signatures enhances data integrity further. Every user on this system has a private key which is unique to him/her and also a public key for signing transactions and verifying them respectively. This way, encryption brings forth authentication, non – repudiation as well as accountability throughout the data transfer process.

X. CONCLUSIONS

While both blockchain and traditional databases have their specific use cases, blockchain's distinct properties of decentralization, immutability, consensus, and digital signatures make it a compelling model for data integrity. Its ability to maintain the originality and trustworthiness of data, even in distributed and untrusted environments, positions blockchain as a transformative technology in the pursuit of secure and reliable data storage and sharing. The potential applications of blockchain for data integrity across different industries and sectors are enormous. The characteristics of blockchain, such as its ability to maintain the originality and security of data, make it suitable for use cases where data trustworthiness is critical, such as supply chain management, healthcare, finance, and legal systems.

However, Scalability, energy consumption (in some consensus mechanisms), and regulatory hurdles are among the key challenges that need to be considered when implementing blockchain solutions for data integrity. Exploring blockchain's role in data

integrity can contribute to the growing body of knowledge, highlighting the potential of blockchain technology to revolutionize data storage and trust among other things.

References

1. Shah, N.K., Bilapate, M., Nandurkar, S., Maalik, M.A., Harne, N., Shaik, K., & Kumar, A. (2023). Efficient Solution for NoSQL Database Security in Blockchain - Based Applications. 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 1-11.

2. Mentsiev, A. U., Magomadov, V. S., Ashakhanova, M. Z., Mentsiev, A. U., & Alams, M. T. (2019, December 1). How the development of Blockchain affected cybersecurity. Journal of Physics: Conference Series, 1399(3), 033048.

3. Habib, G., Sharma, S., Ibrahim, S., Ahmed, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet, 14, 341.

4. Xu, X., Weber, I., Zhao, J., Gu, Z., Tian, Y., & Zhu, H. (2018, August). Trade finance using blockchain technology. In 2018 IEEE International Conference on Blockchain (Blockchain) (pp. 1421-1427). IEEE.

5. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352.

6. Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. (2017, December). BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine, 55(12), 119–125.

7. Lymbouras, A. (2022, July 25). A Shallow Dive Into Bitcoin's Blockchain Part 2 - Transactions. Medium.

8. Watt, A. and N. Eng. (2014). Database Design – 2nd Edition. Victoria, B.C.: BCcampus. Retrieved from

9. Vyawahare, H., Karde, P., & Thakare, V. (2018, August). A Hybrid Database Approach Using Graph and Relational Database. 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE).

10. Sklavos, N. (2014, January 2). Book Review: Stallings, W. Cryptography and Network Security: Principles and Practice. Information Security Journal: A Global Perspective, 23(1–2), 49–50.

11. Saxena, S., & Sharma, M. (2018, October 31). Secure Technique to Achieve Data Privacy and Data Integrity in Cloud Computing. International Journal of Computer Sciences and Engineering, 6(10), 545–548.

12. Lourens, M., Tamizhselvi, A., Goswami, B., Alanya-Beltran, J., Aarif, M., & Gangodkar, D. (2022). Database Management Difficulties in the Internet of Things. 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 322-326.

13. Gopalan, S., Wright, C., & Zadok, E. (2005). Ensuring data integrity in storage: techniques and applications. 26-36. 10.1145/1103780.1103784.

14. Sivathanu, G., Wright, C. P., & Zadok, E. (2005, November 11). Ensuring data integrity in storage. Proceedings of the 2005 ACM Workshop on Storage Security and Survivability.

15. Jensen, D. (2018). Ensure Data Integrity with a proactive Data Management Strategy. View at:

16. Dwivedi, S. K., Amin, R., & Vollala, S. (2023, January). Design of secured blockchain based decentralized authentication protocol for sensor

networks with auditing and accountability. Computer Communications, 197, 124–140.

17. Singh, M., Singh, A., & Kim, S. (2018, February). Blockchain: A game changer for securing IoT data. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT).

18. Park, J., & Park, J. (2017, August 18). Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, 9(8), 164.

19. Guo, H., & Yu, X. (2022). A Survey on Blockchain Technology and its security. Blockchain: Research and Applications.

20. Jiacheng, W., Qingmei, W., & Zheng, W. (2023). Quantitative Dynamic Scalability Model and Analysis of Blockchain Database System. 135-142. 10.1109/DSC59305.2023.00029.

21. Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A.I. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-Peer Networking and Applications, 14, 2901 - 2925.

22. Rawat, B., Purnama, S., & Mulyati, M. (2021). MySQL Database Management System (DBMS) On FTP Site LAPAN Bandung. International Journal of Cyber and IT Service Management.

23. Patil, M.D., & Bhosale, M.V. (2023). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. International Journal of Advanced Research in Science, Communication and Technology.
24. Wei, J., Wang, Q., & Wang, Z. (2023). Quantitative Dynamic Scalability Model and Analysis of Blockchain Database System," 2023 8th International Conference on Data Science in Cyberspace (DSC), Hefei, China, 2023, pp. 135-142,doi: 10.1109/DSC59305.2023.00029.

25. Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to Scalability of Blockchain: A Survey. IEEE Access, 8, 16440- 16455.

Mammu'an Titus Alams holds an MSc in Computer Security and Forensics from the University of Bedfordshire, UK (2015), and a BSc in Computer Science from the University of Jos, Nigeria (2012). He is currently a lecturer in the Department of Computer Science at the University of Jos.
Alams is a member of the Internet Society (ISOC), with research interests spanning cybersecurity, digital forensics, blockchain technology, and machine learning. He also has hands-on experience in cloud computing, blockchain systems, Linux system administration, ethical hacking, virtualization technologies, database management systems, and scripting for automation using Python and Bash.

Godwin A. Thomas (Dr) Earned his PhD in IT at the Nelson Mandela University Port Elizabeth, South Africa in 2014. Prior to that he earned his BTech in 2006 and subsequently his MTech (cum laude) in 2007 at the same University. He currently works as a Snr Lecturer in the Department of Computer Science at the University of Jos in Nigeria, where he had previously earned his National Diploma in Computer Science in 2001. He is currently a member of the Internet society (ISOC), and Nigerian Computer Society (NCS). His research interest include Computer support cooperative work (CSCW), Information security governance, Mobile Computing and IT service management. He is ITIL certified.

Stephen Mallo JR obtained his BSc in Information Technology in 2011 at the Eastern Mediterranean University then later went back to the same University to earn (Merit) Mtech in Information Technology 2019 in Eastern Mediterranean University North Cyprus (TRNC), Turkey. He is Cisco Certified Network Associate (CCNA) certified. and currently a lecturer in the Department of Computer Science at the University of Jos Nigeria. He is currently a member of the Internet society (ISOC) and Institute of Electrical and Electronic Engineers (IEEE). His research interests are Information Technology, Networking, Artificial Intelligence, Machine Learning, Internet of things (IoT), ICT equipment and gadgets for Security.
David Enekai Oguche Earned his MSc in Internet Computing and Network Security at Loughborough

University, UK in 2013. Prior to that he earned his BSc in Computer Science in 2012 at the same University. He currently works as a Lecturer in the Department of Computer Science at the University of Jos in Nigeria. He is currently a member of the Internet Society (ISOC). His research interests include Artificial Intelligence, E-health, and Big Data.

Betty Toyin Dimka is currently pursuing her PhD at University of Jos. She earned her B.Sc. in 2015 and subsequently her MSc.in 2023 at the same University. She currently works as a Lecturer in the Department of Computer Science at the University of Jos in Nigeria. She is currently a member of the Nigerian Computer Society (NCS). Her research interests include Data Science, AI, And Mobile Computing.