|| Volume 9 || Issue 6 || June 2025 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

BLOCKCHAIN-BASED SECURITY SOLUTIONS FOR ENSURING DATA INTEGRITY AND PRIVACY IN BIG DATA SYSTEMS

Anil Kumar Jakkani
Research Consultant, The Brilliant Research Foundation, India
anilkumar.svnit@gmail.com

----------***----------

Abstract: The reason why conventional forms of security fail to address the issues of fluctuating big data systems space adequately. Instead, the use of blockchain technology which is a decentralized and entirely transparent and unalterable can provide a proper solution toward these problems. Based on the above Introduction, this paper aims at discussing the application of implementing blockchain security in big data systems. In other words, if data is stored using blockchain, it is very easy to prove as to whether the data has been manipulated or not. Due to the distributed nature of the blockchain, there is also a consideration of the fact that it eliminates the possibility of having single points of failure as a weakness for big data systems. In addition, smart contracts on the blockchain platform can fulfill and enforce data governance policies and regulatory compliance. This paper also presents an analysis of the state of the art of the existing blockchain-based security solutions, their strengths and weaknesses and a vision of the opportunities for further research. The combination of aspects of blockchain technology and big data systems means the possibility of radical changes to data processing to heighten confidence and security in the processing of valuable and security-sensitive data.

Keywords: *Blockchain, Data Integrity, Privacy, Big Data, Security.*

----------***----------

I.INTRODUCTION:

In the past decades, big data has central for the organization and different sectors where they used it in innovation, decision-making process, and competition. However, the large and ever growing size of the big data present this couple of challenges within systems; quality and security. When it comes to these complexities, traditional security approaches generally fail to provide the necessary level of protection to the data which may be stolen, changed, or accessed by unauthorized people. In this regard, it has emerged the need for appropriate security systems so as to guarantee the defence of big data systems, however still preserving the data's purity as well as the customers' privacy.

New generation solutions such as blockchain which comprises of decentralized, transparent, and immutable features pose an excellent solution to these challenges. Blockchain which started as the underlying technology for cryptocurrencies has expanded and is now used for other purposes such as data protection and security. Through the advanced use of blockchain, the big data systems in organizations will be made more secure to retain the big data in a tamper-proof manner and limit the access of such data to only authorized personnel. This paper aims to provide a review on the trending technologies of blockchain based security solutions for the big data systems with respect to their features, drawbacks, and scope of future research.

1.1 Blockchain Technology Overview

Blockchain is an open source distributed ledgering system that records transactions in a more secure and an efficient way that responds to cases of fraud by making it very difficult for an individual to alter the information that is contained in the block chain. In the chain every block is comprised of transactions while every block is linked to the previous one by using a cryptographic hash. This structure makes it impossible for anyone to attempt to change a block as this will impact the rest of the blocks thus making the data non-restorable. This makes it possible to eliminate the requirement of a central controller, as all the participants of the blockchain networks manage the ledger.

Another aspect of blockchain is the consensus layer which guarantees that all the stakeholders approve the verification of transactions before they are incorporated as blocks into the chain. It is done using different algorithms for example the proof of work (PoW) or the proof of stake (PoS) act as barriers to the fraudsters who want to corrupt the databases. Furthermore, it contains the use of dispersed ledger as well as cryptography in a manner that will protect the identity of the participants in a transaction.

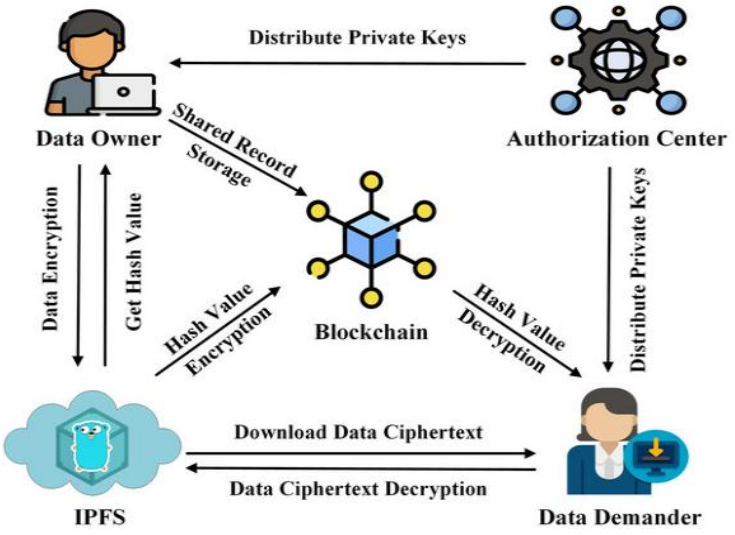

Figure 1: *System architecture*.

This paper has found that blockchain offers numerous possibilities for improving integrity and privacy of big data that stem from its key

characteristics of decentralization, transparency and immutability. By recording data over a block chain, the organization or company can be sure that the data has not been modified in any way and if it had there would be a way of telling whether the data was changed or not. In addition, the use of a block chain's cryptographic properties can facilitate the development of secure, authorisation based access schemes. A blockchain based traceable and secure data sharing scheme is depicted in Figure 1.

1.2 Data Integrity in Big Data Systems

The another significant issue concerning BIG Data is data integrity, which defines the dataset's quality due to the absence of imperfections and inaccuracies. However, keeping the integrity of the data within the big data environments is not easy due to the volume and the velocity of the data. Checksum or digital signatures may not act as reliable solutions on large-scale systems to avoid tampering of the collected information.

This is much more reliable way of maintaining data integrity in big data systems through the use of blockchain technology. This means that when data is stored on a blockchain, all the data is connected through a cryptographic hash and form a chain of records which cannot be altered. The alteration of the data will disrupt the data chain and the tampering will at once be recognizable. This feature of blockchain prevents the alteration and deletion; thereby providing an accurate record of the information in the blockchain.

Moreover, the use of blockchain leads to the possibility of using smart contracts that are contracts in which the terms of the agreement are integrated into the code. Smart contracts can help execute and enforce the policies and rules for data, meaning that data will always be managed in a specified manner. These types of automation minimize human factors and improve the credibility of big data systems in being more accurate. One of the previously proposed model for blockchain-based data integrity authentication technique is shown in Figure 2.

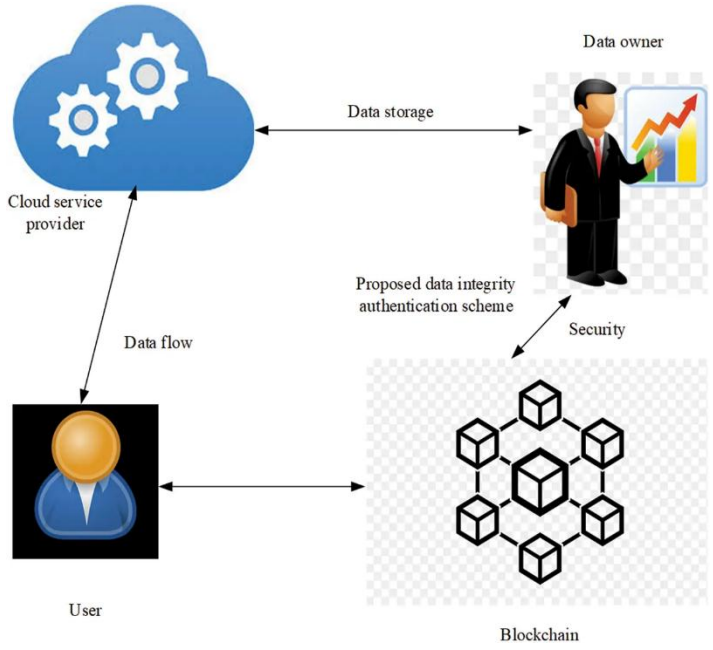

Figure 2: *Previously Proposed Block Diagram*

1.3 Data Privacy in Big Data Systems

Another major issue that can be associated with big data systems is data privacy since big data is often characterized by the large amounts of data collected, stored and processed in the system that in turn may be accessed by the unauthorized subjects and misused. Some of the more traditional approaches to protecting data include the use of encryption and access control mechanisms and these may prove to be inadequate in case of large-scale systems where the risk of breaches is comparatively greater.

To the digital privacy in big data systems, blockchain technology offers a more secure and a more transparent system. Through blockchain, it is possible for an organization to put in place sound access control measures that would only allow specified parties to have access. Some of these mechanisms can be implemented using automated administrative mechanisms where smart contracts can be used I verifying the rights of access to the information.

Secondly, the operate of blockchain also supports the adoption of more complex cryptographic mechanisms, for instance, zero-knowledge proofs and homomorphic encryption mechanisms. These techniques enable data to be manipulated and analyzed while keeping the sensitive information on which the operations are performed out of sight thus preserving the privacy of data in big data scenarios.

1.4 Advantages of Blockchain-Based Security Solutions

As seen from the above discussion, blockchain based security solutions have the following benefits in protection of data integrity and privacy in big data system. This is due to the ingenious structure of blockchain; this is a type of database that does not require centralization of an authority hence minimizing single points of failure. This decentralized system improves the security firmament of the big data systems and makes such systems less vulnerable to attacks and breaches.

Transparency claim the second benefit for utilizing blockchain-based security solutions. The inherent characteristics of blockchain –Immutability and the non–alterable features make it possible for all records of transactions to be seen and modified using the blockchain. This creates credibility especially to all the stakeholders so that he or she can notice any unlawful activities or attempts to interfere with the system.

In addition, the applications of blockchain in rendering security solutions for big data are immensely scalable to serve the versatility and volume of big data systems. The blockchain consensus mechanisms speak of its versatility when it comes to management of the large quantity of information as the system evolves without compromising on the security of the information.

Nevertheless, like any other decentralized technologies, there are certain drawbacks of using blockchain to develop security solutions. The first drawback is the scalability issue, this is because the presently existing blockchain technologies may not support large volumes of transactions and volumes of data needed in big data systems.

Further research has to be carried out to invent better consensus

approaches and data archiving methods that can be utilized in large-scale settings.

Another disadvantage may be seen in the compatibility problem between the blockchain systems because sometimes they cannot be interconnected with the existing big data systems. The future work in regards to the problem should concentrate on the creation of the standardized solutions to integrate various blockchain and big data structures.

Also, the standards for utilising blockchain technology for security solutions are relatively new with the need for guidelines as well as for data protection regulations. It is also useful to consider further studies of legal and regulatory frameworks for further application of security based on blockchain technology and identification of guidelines for the introduction of such technology in big data systems.

II.REVIEW OF WORKS

Blockchain has now been recognized as one of the viable technologies for tackling problems associated with big data such as data integrity and privacy. This paper aims at reviewing the literature on the state of the art of blockchain-based security for the big data systems and key insights, methods and future works discussed. In line with the objective of this review, the roles of different authors are discussed with a view of helping the reader understand the pros and cons of using blockchain in the big data situations.

Blockchain has for example been regarded as a revolutionary technology for a number of industries, and big data is no exception. In the paper by Yu (2016) the authors shared their views and possibilities for privacy in the big data context underlining the significance of proper data protection. Data privacy and control was pointed out as an important aspect on big data systems which was well illustrated by the author. Along the same vein, Soria-Comas and Domingo-Ferrer, (2016) discussed the threats to privacy principles and models in big data and called for higher order protection solutions for the big data.

Additionally, decentralization of the blockchain affords the primary advantage of dispensing with the necessity of a central authority making it ideal for big data systems. Zyskind and Nathan underlined, that with help of blockchain it is possible to create a decentralized personal data management system, their work clear showed the idea about how blockchain can effectively work in the sphere of personal data management. Their work explored the risks and opportunities of blockchain in big data focusing on the possibilities to improve data ownership and privacy. Further, Conoscenti et al. (2016) presented a systematic literature review with respect to the use of blockchain in IoT context which contributes a huge amount of big data. In their work, blockchain's decentralised nature was seen to be a key factor in overcoming the obstacles to data authenticity and confidentiality in IoT settings.

The preservations of data integrity is a major concern in big data system and blockchain technology presents a way to preserve the integrity of data. Nakamoto (2008) began the discussion on blockchain by publishing the Bitcoin white paper where he stressed on the fact that any alteration of the blockchain is easily identifiable since the chain maintains an unchangeable record. It is also very useful for ensuring data consistency for big data systems; a characteristic that makes it essential. In the same vein, Aitzhan and Svetinovic (2016) analyzed how blockchain may be applied in decentralised energy trading where they stress on the attribute of the ledger of blockchain on non-modifiable.

Furthermore, it is possible to deploy smart contracts on the blockchain to address data management governance polices. Warren (2012) did come up with Bitmessage which is a peer to peer message authentication and delivery system and this shows how blockchain can ensure data integrity by use of automated rule based systems. Furthermore, McMyn and Sim (2017) explained how blockchain can help improve data values in financial systems since the use of blockchain creates a more secure and transparent way of tracking data.

Security is an important issue in big data and the adoption of blockchain help in providing better security measures to the data. In the earlier article, Lindsey (2017) also considered the problems of data privacy as one of the key concerns for IoT and underlined the necessity of more efficient protection tools. The author also stressed that blockchain technology could provide improved data protection of IoT networks. In the same way, Zyskind and Nathan (2015) presented a decentralized personal information management system employing the use of blockchain where they showed an instance of how blockchain is well suited in managing personal information in the big data structure.

In addition, the sets of characteristics of the blockchain solve the ability to use sophisticated, high-level encryption, including zero-knowledge proofs and homomorphic encryption. Such techniques enable the data to undergo computations and analyses while concealing the raw data which is often very sensitive thereby protecting the privacy of the data in big data systems. Lin & Liao, 2017 have presented a survey of the key security concerns and threats related to blockchain with the need for improving the data privacy by implementing more sophisticated encryption methods. Also, Gorkhali et al., (2020) discussed the literature on blockchain and focusing on the possibilities to further apply the cryptographic characteristic of blockchain towards the improvement of data privacy in big data systems.

Based on the ideas of blockchain, there are a number of ways or advantages when it comes to security solutions in big data systems. There is no doubt that decentralization is one of the biggest talking points when it comes to blockchain technology because it helps to minimize the risk of single points of failure. As much as Yu (2016) considered the effectiveness and the drawbacks of the concept of privacy concerning the utilization of the big data, the author emphasized that distributed solutions can be useful in the improvement of the security of big data. Likewise, Soria-Comas and Domingo-Ferrer in their work detailing the tensions to privacy principles and models in big data highlighted the limitations of security in and called for decentralize security to counter the risks of consolidating data banks.

The last benefit of using blockchain for security solutions is its transparency that simplifies tracking of all the operations. The open, permanent and unalterable characteristics of the blockchain guarantee that all operations and records changes are transparent and can be seen by all the members. Nakamoto (2008) introduced the use of blockchain by presenting the idea in the information provided on the bitcoin website, and explained that each block in the chain is public and allows anyone to view all the activities taking place in the system and any attempt to manipulate the data to favor certain parties would be easily detected. Furthermore, Aitzhan and Svetinovic (2016) discussed the application of blockchain for creating decentralized energy markets while highlighting the need for the blockchain consensus protocol to allow decentralised data sharing without compromising the privacy of data.

On the pluses of the blockchain-based security solutions it is possible to note a number of benefits, but there are some shortcomings that should be discussed. There is also the scale issue which could be a problem as most of the current blockchain technologies are not capable of handling large number of transactions and data processing capabilities of big data. A summary of the various insights that were compiled in the review by Yli-Huumo et al. (2016) highlighted the scalability issues that arise in blockchain technology especially concerning the consensus mechanisms and the data storage strategies. Similarly, the security challenges and prospects of blockchain system were compiled in the survey conducted by Lin and Liao (2017) and indicated that while implementing the security solutions on blockchain, scalability issues are prominent.

One last drawback is the problem of homogenization due to which integration of different blocks on the blockchain platforms can be incompatible with big data systems. A systematic literature review that relates to implementation of blockchain for the Internet of Things (IoT) by Conoscenti et al. (2016), revealed that there is a need for standards and protocols that support interoperability between blockchain and big data systems. Finally, there are no well-defined legal frameworks that provide for blockchain based security solutions and there is a lot of uncertainty about what kind of mechanism has to be implemented so that the systems are compatible with the data protection laws. In his literature review, Gorkhali et al. , 2020 also emphasized the need to find a clear set of guidelines regarding the use of the blockchain as a security approach.

Thus, the literature review reveals the prospects for the application of blockchain-based security for protecting the integrity and confidentiality of big data systems. Through the use of blockchain, which is decentralised, transparent and has an attribute of immutability, organisation can improve on the security of big data to increase trust and transparency to sensitive and valuable information. However, to realise the full potential of security through blockchain, additional research has to be carried out regarding the scalability of blockchain, how these different blockchains can interoperate, as well as the legal implications of using blockchains for security.

III. PROPOSED METHODOLOGY

This paper uses a documentary review and qualitative techniques to examine the risks and possibilities of privacy in big data context. The research method aims at giving a clear insight on the current state of endangerment of privacy, the effects of big data technologies and the available solutions to the problem of data privacy. Despite this, the research does not involve participating in experimental procedures of any kind, but the synthesis and critical evaluation of the literature, as well as opinions of experts in the field.

The first process in the methodology involves a conduct of a systematic literature review. It starts from searching and selecting of articles, reports, white papers that are focused on the discussion of big data and privacy. The following technical databases named IEEE Xplore, Google Scholar are some of the databases that respond to specific search words like “big data privacy”, data protection”, “blockchain technology”, and “consumer privacy” are searched and also it does not restrict the search of the publications by the year of publication though latest discovered research papers are encouraged.

After the literature search, all the materials that have been retrieved are sorted to identify those which are most relevant to the study and of good quality. The following articles are then chosen for a comprehensive analyze; the articles that match up to the laid down criteria. The criteria for selecting articles include: The topic, the author’s credibility, and finally, the extent to which the articles cover the issue of privacy and big data. The chosen literature is then classified according to the topic areas, including privacy issues, technology-based approaches, ethical issues, and legal requirements. Classification also assist in sorting of information and come up with some of the significant areas of concern.

The methodology used for conducting the qualitative analysis consists in the critical appraisal of the chosen sources. From the literature, related themes or patterns are noted down and synthesized in a logical manner in order to come up with an overall understanding of the privacy issues prevalent today while operating in the world of big data. It also presents a contrast of the various views and strategies concerning privacy protection and the advantages or disadvantages of each of them. Also, there is also included the analysis of cases and examples to support the discussion of problems and solutionsrelated to privacy issues and outcomes of suggested measures. Finally, the results of this study are discussed and integrated so that understanding of the research area as well as revealing the overall prospects can be provided and issues in big data privacy and identify the probable courses of action in the area of big data privacy, which can be helpful for devising future research directions and policies.

IV. RESULTS AND DISCUSSION

4.1 Lessons for Privacy in the Era of Big Data

From the literature review, there was emerged several key privacy concerns brought about by the adoption of big data technologies. Among the challenges the first one is the excessive collection and storage of PII by organizations, which in turn raises the likelihood of data leaks and breaches. Furthermore, due to the large volume,

source and variety, big data raise high risks in anonymizing data and eliminate re-identification of people. The latter is particularly alarming given that utilising sophisticated analytics and machine learning algorithms only aggravates these problems by allowing to obtain valuable individual details based solely on the available data that would seem commonplace at the first glance.

4.2 Technology based strategies for privacy protection

This paper discusses various technological solutions that have been proposed to overcome the privacy issues in big data. One such technique is the Differential Privacy that introduces 'noise' into data in a bid to promote individual's privacy while not compromising on the general analysis of aggregated data at the end-user level. Another solution is homomorphic encryption through which computations are performed over encrypted data thus enhancing security of data. Additionally, it is agreed in the literature that blockchain offers the potential for greater privacy by the decentralised management and sharing of data.

4.3 Ethical consideration and Consumers perceptions

The violation of big data privacy has been undertaken as ethical consideration in the extant literature. Concerns about ethical use of personal data are increasing, for such aspects as consent, transparency and accountability. The consumer is now wiser to realizing the worth of his/her data, and thus, expects organizations to practice proper handling of data. literature also points to standards and ethical codes so that data collection and usage are appropriate and satisfactory to the society.

4.4 Role of Governments and Regulatory Mechanism

A survey of the various regulatory bodies in the world shows that there is a tendency of policies becoming more stringent when it comes to the protection of data. The GDPR in Europe and the CCPA in the United States are specific pieces of legislation focusing on the protection of individual's right to privacy. These regulations traverse deep standard for controllers and processors such as permanent and minimal data, limited usage, special user control, etc. research also points out that it will be possible to enhance the level of privacy protection by enhancing the implementation of these regulations in the big data environment.

4.5 Examples of five platforms taken from real life.

To show and discuss the practical applications of privacy issues as well as the efficiency of the discussed solutions, several case studies and real-life examples were provided. For instance, The implementation of the blockchain technology in decentralised energy trading systems has been seen to offer benefits in the area of privacy and more so security. In the same way, use of privacy protection measures has allowed for the exchange of sensitive health data without compromising the privacy of the patients. The above cases show how PETs can be adopted in different industries and why the use of the technologies is practical to enhance privacy protection.

In conclusion, results of the research pointed towards the complexity of the privacy issues regarding big data and the necessity to address those issues on many levels: technological, ethical, legal, and in terms of application. The study shows that there is need for constant reviews and development of solutions to counter the ever-changing privacy trends in the use of big data technology

V. CONCLUSION

Big data and privacy is a vast area filled with an ever-developing array of issues and opportunities as well as one that has a plethora of challenges. The conclusions of current paper stress the necessity of proper technological applications, ethical standards, and legislatives to uphold private information security regarding the further advancement of the data technologies. This finds application in, differential privacy and homomorphic encryption as methods that have the potential to enhance protection of data and blockchain technology aspect which is likely to shape the future practices of data protection. The enactment and effectiveness of the modern and global data protection laws like GDPR and CCPA contributes towards underlining people's rights to privacy.

Indeed, it can be noted summarizing that it is essential to focus on the combination of advances in technology, ethics, and law when it comes to the protection of privacy in the context of big data. The research in the future should build and reshape international privacy technologies and analyze the moral use of data together with examining the success of the government rules and regulations. Moreover, there is a need for cooperation between academicians, industry, and policy makers so that the culture of using big data appropriately that is in a responsible way is adopted, people's privacy rights are protected and benefits of big data can be achieved. There is nothing wrong with big data privacy if it is managed appropriately as will be shown by taking a well rounded and proactively approach to the challenges presented by big data.

VI.REFERENCES

[1]. Yu, S. (2016). Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data. IEEE Access, 4, 2751-2763. https://doi.org/10.1109/ACCESS.2016.2577036

[2]. Lindsey, N. (2017, March 17). Data Privacy in the Era of the Internet of Things. CPO Magazine. https://www.cpomagazine.com/data-privacy/data-privacy-era-internet-of-things/

[3]. Soria-Comas, J., & Domingo-Ferrer, J. (2016). Big Data Privacy: Challenges to Privacy Principles and Models. Data Science and Engineering, 1, 21-28.

[4]. Adwani, Arun. "Fintech Innovations and Financial Resilience: A Framework for Crisis Management." Available at SSRN 5201781 (2025).

[5]. Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[6]. IEEE TRENDS. (2017). Top technology trends 2018. Computer. https://www.computer.org/press-room/2017-news/top-technology-trends-2018

[7]. Conoscenti, M., Vetrò, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). Agadir, Morocco.

[8]. Adwani, Arun. "The Role of AI and Big Data in Enhancing Financial Risk Assessment Models." Available at SSRN 5201777 (2025).

[9]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[10]. Gowda, V. Dankan, Annepu Arudra, K. M. Mouna, Sanjog Thapa, Vaishali N. Agme, and K. D. V. Prasad. "Predictive Performance and Clinical Implications of Machine Learning in Early Coronary Heart Disease Detection." In 2024 2nd World Conference on Communication & Computing (WCONF), pp. 1-8. IEEE, 2024.

[11]. Aitzhan, N. Z., & Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing.

[12]. Adwani, Arun, FOUNDATIONS OF FINTECH: NAVIGATING THE DIGITAL FINANCIAL REVOLUTION (January 28, 2025). Available at SSRN: https://ssrn.com/abstract=5133519 or http://dx.doi.org/10.2139/ssrn.5133519

[13]. McMyn, A., & Sim, M. (2017). R3 Reports with Hogan Lovells.

[14]. Warren, J. (2012). Bitmessage: A peer-to-peer message authentication and delivery system.

[15]. Adwani, Rabail. "Innovative Financing Models for Startups: Challenges and Opportunities in a Globalized Economy." Available at SSRN 5162026 (2025).

[16]. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.

[17]. Adwani, Rabail. "Blockchain Applications Beyond Cryptocurrency: Transforming Industries." Available at SSRN 5162028 (2025).

[18]. Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653-659.

[19]. Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: A literature review. Journal of Management Analytics, 7(3), 321-343.

[20]. Gowda, Dankan, D. Palanikkumar, A. S. Malleswari, Sanjog Thapa, and Rama Chaithanya Tanguturi. "A Comprehensive Study on Drones and Big Data for Supply Chain Optimization Using a Novel Approach." In 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), pp. 1-7. IEEE, 2024.

[21]. S. S. Gujar, "Blockchain-Based Framework for Secure IoT Data Transmission," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910705.

[22]. S. S. Gujar, "Machine Learning Algorithms for Detecting Phishing Websites," 2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICSES63760.2024.10910759.

[23]. Adwani, Arun. "The Evolution of Digital Payments: Implications for Financial Inclusion and Risk Management." Available at SSRN 5201787 (2025).

[24]. Adwani, Rabail, and V. Sudhakar Rao. "Decentralized finance (defi): Reshaping traditional banking systems." European Economic Letters, 0 [10.52783/eel. v15i1. 2432] (2025).

[25]. Ahmed, Amjed A., et al. "Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks." IEEE Access (2024).

[26]. Nagarajan, Sevinthi Kali Sankar, et al. "Enhanced Anomaly Detection in Embedded Payment Systems using Depthwise Separable CNN with Dandelion Optimizer." 2025 International Conference on Intelligent Computing and Control Systems (ICICCS). IEEE, 2025.

[27]. Ahmed, Amjed Abbas, et al. "Detection of crucial power side channel data leakage in neural networks." 2023 33rd International Telecommunication Networks and Applications Conference. IEEE, 2023.

[28]. Adwani, Rabail. "Evaluating the Risk Management Strategies of Global Banks in the Digital Age." Contemporary Challenges in Multidisciplinary Research: A Collaborative Approach 1.37 (2025): 391-404.

[29]. Ahmed, Amjed Abbas, et al. "Optimization technique for deep learning methodology on power Side Channel attacks." 2023 33rd International Telecommunication Networks and Applications Conference. IEEE, 2023.

[30]. Sadiq, Ahmed Tariq, Amjed Abbas Ahmed, and Sura Mazin Ali. "Attacking classical cryptography method using PSO based on variable neighborhood search." International Journal of Computer Engineering and Technology 5.3 (2014): 34-49.

[31]. Muhammad, Ammar Abdulhassan, et al. "Adaptive Optimization of Deep Learning Models on AES based Large Side Channel Attack Data." Alkadhim Journal for Computer Science 2.1 (2024): 72-85.

[32]. Ahmed, Amjed Abbas, and Mohammad Kamrul Hasan. "Multi-layer perceptrons and convolutional neural networks based side-channel attacks on AES encryption." 2023 International Conference on Engineering Technology and Technopreneurship (ICE2T). IEEE, 2023.

[33]. Madhloom Kurdi, Waleed Hadi, et al. "Efficient Two-Stage Intrusion Detection System Based on Hybrid Feature Selection Techniques and Machine Learning Classifiers." International Journal of Intelligent Engineering & Systems 18.3 (2025).

[34]. Muhammed, Ammar Abdulhassan, Hassan Jameel Mutasharand, and Amjed A. Ahmed. "Design of deep learning methodology for AES algorithm based on cross subkey side channel attacks." International Conference on Cyber Intelligence and Information Retrieval. Singapore: Springer Nature Singapore, 2023.

[35]. Ahmed, Amjed Abbas, et al. "Efficient convolutional neural network based side channel attacks based on AES cryptography." 2023 IEEE 21st Student Conference on Research and Development (SCOReD). IEEE, 2023.