International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# Securing CCTV Video through Blockchain

**S.V Gunjal[1], Arti Chavan[2], Ashwini Dhawale[3]**

*[1]Professor, Dept. of Cloud Computing and Big Data, P.Dr.V.V.P. Institute of Technology and Engineering, Loni,*
*Maharashtra, India*
*[2,3,4] Final year Diploma Student, P.Dr.V.V.P. Institute of Technology and Engineering, Loni,*
*Maharashtra, India*

---

**Abstract -** Blockchain technology has grown from becoming an immutable database of transactions for crypto currencies to a programmable interactive environment for creating distributed reliable applications. While, blockchain technology has been used to solve numerous problems, to our knowledge none of the previous work centered on using blockchain to build a stable and immutable science data provenance management system that automatically verifies the provenance records. In this job, we use blockchain as a medium to promote trustworthy data provenance compilation, verification and management. Due to the lack of successful storage mechanism, incidents that allow the CCTV Video to be forged also get noticed. In order to address this problem CCTV Video systems are adopted even though security problems are still remaining. Blockchain is one of the most recent technologies that can be used for the data protection. The irreversible property of the block chain helps to solve the problem of CCTV Video forgery.

***Key Words***: Blockchain, CCTV Video, Security.

## 1.INTRODUCTION

CCTV Video contain material private to the people and cannot be readily available to anyone. Hence, there is a high need for a system that can ensure that the material in such a CCTV video is original, which ensures that CCTV video has come from an authenticated source and is not false. In addition, the material in the paper should be secret so that it can only be accessed by designated individuals.

Blockchain technology is used to minimize the occurrence of CCTV video forgeries and ensure that the reliability, legitimacy and confidentiality of CCTV video can be enhanced. Technologies occur in related fields, such as digital fingerprints, which are used in CCTV video to provide verification, credibility, and nonrepudiation. However, for the specifications of an CCTV video, it has crucial security gaps and missed functions: for example, it uses the keys to validate the alteration of the record, but doesn't initiate the validation of the public key CCTV video status immediately.

This can result in a forgery being accepted if the key has been compromised. Furthermore, also the signer's public key credential has been authenticated, but the signed paper itself hasn't. In our case with an CCTV Certificate, the signed form itself is also a CCTV video, and could have a legitimate duration.

CCTV video which adopts digital signature technology, presents to the user by the authority to validate the user himself in the digital fields used to confirm a user's identity and access authorization to the network resources. CCTV video can be extended to e-commerce operations on the internet and e-government activities, whose domain get interested in application of identity verification and data protection, like conventional financial, manufacturing, retail online purchases, public services etc.

Blockchain is the fundamental era underlying the rising crypto currencies along with Bitcoin. the key gain of blockchain is extensively taken into consideration to be decentralization, and it is able to assist set up disinter mediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual believe and centralized control amongst character nodes, based on such strategies as information encryption, time-stamping, disbursed consensus algorithms, and monetary incentive mechanisms. As such, blockchain can offer a unique solution to the longstanding issues of high operation expenses, low performance and potential protection risks of statistics garage in conventional centralized structures.

[1] Nikhil Bhusari et al. describes the methodology for an effective approach for the purpose of integrity evaluation has been outlined in detail in this research article. Videos are highly useful and have been an effective part of everyday human life in the recent years. While most of the smartphones are effectively

equipped with the state-of-the-art camera sensors that can effectively capture a video, most of the videos that are captured are in the form of video surveillance. Videos are so important that they are used as evidence in the court of law to achieve effective and useful incrimination against the criminal. For this purpose, the system takes the video as an input which is effectively utilized for the frame extraction. Once the frames of the video are extracted these frames are effectively encrypted through the use of RSA encryption system. These encrypted frames are transferred to the next module which is the key generation
module. This module effectively generates the keys of the encrypted frames which are then utilized the successfully to build a blockchain platform.

[2] A. Fitwi et al. explain security and privacy are very essential issues in the world of video surveillance. Hence, this paper proposes SePriS, a private blockchain based solution coupled with an efficient video frame enciphering mechanism for sharing stored surveillance videos in a secure and privacy-aware way. It illustrates how the blockchain technology can be leveraged to prevent abuse and leaking of stored videos, which have plagued the surveillance practice for years. The experimental analysis show that the video frame enciphering mechanism passes the standard computational and security parameters. Additionally, they corroborate the security, privacy, integrity, authenticity, controllability, auditability, and accountability of the proposed decentralized system for sharing of stored surveillance videos. Overall, the SePriS system achieves the design goal and creates a video surveillance system with good balance ofprivacy and usability.

[3] Min-Hyuk Jeong et al. introduced an IoT camera video streaming scenario was proposed and was implemented the IoT camera video streaming system that operates. With standardized APIs and smart contracts in blockchain 2.0, the DApp can access IoT cameras on the Internet and receive video streaming services regardless of platform. author examined off-chain transactions to overcome a low TPS and support a proper refund mechanism when service errors occur. By comparing the three off-chain transaction methods, author selected the state channel method as the most suitable off-chain transaction for the IoT camera video streaming system. A new video streaming system scenario was proposed by applying the state channel method to the IoT camera video streaming system.

This paper's second portion provides an analysis of the previous studies that were considered as Litereature Survey. In Section 3, the course of action is described in full detail as Proposed methodolgy. Part 4 digs into the experimental evaluation, while Section 5 explores potential changes before wrapping up the article with a conclusion on the current proposal.

## 2. LITERATURE SURVEY

[4] Eryk Schiller et al. narrate about the first access management system, which utilizes Artificial Intelligence (AI), Blockchains(BC), and Internet-of-Things (IoT) in an integrated use-case. Thus, the user needs to present his/her face in front of a camera to access a resource. The system takes the image of that person and checks, whether this given user has the right to access a given resource. Face detection and recognition are performed directly on the IoT device. To detect faces, a MT-CNN (Multi-Task Cascaded Convolutional Network) with Mobile Nets (MN) was deployed. Furthermore, the Face Recognition model is based upon a Convolutional Neural Network (FRMN). To establish a good level of transparency, the AI decisions on access rights as well as images taken by the sensor are stored in the immutable, tamper-resistant storage implemented with the help of the Hyper Ledger Fabric (HLF).

[5] D. Na et al. describe the oracle problem and data privacy, i.e., the existing challenges when using blockchain technology, so as to ensure the reliability of Dash cam video data. To solve the oracle problem, the vehicle connected to the V2V network is grouped based on GPS data, and a client for transmitting the transaction to the blockchain is selected from among the nodes. The client collects the transaction and stores it in the blockchain; multiple image data are stored for a scene. In addition, the performance of the proposed overall system is measured, and it is confirmed that the latency in the proposed structure does not have a significant effect on the overall system. However, in this study, (1) capacity increase due to multiple signatures recorded on the blockchain (2) vehicle IoT devices cannot participate as a blockchain node (3) There is a limit to verifying the reliability of GPS data.
Limitation\Future Scope: In future research, author plan to study multi-signature compression method, consensus algorithm, lightweight block chain applying block weight reduction method, and RSU-based vehicle grouping method.

[6] Moolikagedara, K. et al. presents a video blockchain framework that validates the hypotheses formulated in the study. The results underscore the significant enhancement in security and data integrity achievable through the utilization of a video blockchain within smart city surveillance systems. This outcome posits that the integration of a video blockchain establishes a robust security mechanism for the storage and retrieval of surveillance camera video records. The combination of vehicle cameras, blockchain technology, and third-party certification authority (CA) verification ensures the secure and sequential storage of video data, protecting it against tampering and unauthorized access. Lastly, the proposed video blockchain approach effectively mitigates the risks associated with malicious attacks, data tampering, and privacy violations in surveillance systems, enhancing their effectiveness in crime scenarios. This paper contributes to the field by establishing a link between video frames captured by intelligent surveillance systems and blockchain. By leveraging cryptographic functions and decentralized storage platforms, the security of vehicle camera transferring video data is significantly improved. The proposed blockchain-based approach not only enhances the security and integrity of vehicle video data but also promotes trust, reliability, and controlled disclosure in smart cities.
Limitation\Future Scope: Taking into account these limitations, author plan to extend our research in future endeavors to enhance the system's resistance against attacks from quantum computers. This approach is of significant value to law enforcement monitoring, autonomous vehicles, insurance providers, and traffic management systems, providing increased security and adaptability for an advanced vehicular distributed video network in smart urban environments.

[7] Y. Ding et al. proposed a secure and manageable VoD stream distribution scheme based on hybrid P2P CDN by integrating permissioned blockchain and zk SNARK. Therein, to prevent arbitrary tampering of the video in distribution and verify its integrity, the original video was partitioned into a series of small-sized segments, each committed to building a Markel tree of that video. Additionally, for peer-to-peer authentication, author eliminated the need for traditional public certificates by introducing AC to aid the mutual authentication among content requesters and content providers. The security evaluation demonstrated that our proposed P2P-CDN could achieve security and privacy protection.
Future Scope: In future work, author would like to introduce an incentive mechanism in consensus, which could benefit the enthusiasm of validating peers and discourage their malicious behavior.
Limitations- Experimental data show that the performance of blockchain systems incorporating zero-knowledge proofs is closely related to the number of P2P network peers. However, due to the limitation of the simulation environment and configuration, author cannot test more peers to get closer to the actual data because the number of real-world network peers counts in tens of thousands.

[8] Hira et al. introduced a blockchain is a new concept, and to researchers; knowledge, a study on the blockchain VDOT mHealth app has not been conducted yet. This empirical study, therefore, fills the knowledge gap. UTAUT variables have not been sufficiently tested in a blockchain-based health application context. The present study has made a valuable contribution by examining UTAUT factors in explaining users' readiness for blockchain-enabled mobile app. It explores moderating the influence of age and gender on the direct relationship of the model. Age and gender do not condition patient's behavior intention to use the blockchain VDOT mHealth app. The policymakers need to set policy keeping in consideration that perceived benefit and initial trust building are of utmost importance.

[9] Sartzetakis Nektarios et al. explain that research has demonstrated that integrating blockchain technology into video ad serving can bring numerous benefits to all stakeholders involved. Advertisers can gain increased trust and accountability by verifying ad impressions and ensuring that their content is being served to genuine users. Publishers, on the other hand, can benefit from improved revenue potential through the elimination of ad fraud and enhanced targeting capabilities. VidAdChain is an innovative research project that is in the process of designing a prototype, blockchain enabled, video advertising management and delivery system. In this stage of the research endeavor, the algorithmic design of the system has progressed, and the main challenges/barriers to implementation have been identified. VidAdChain is currently addressing these challenges and aims to demonstrate by the end of the project's duration a working prototype solution for a blockchain-enabled digital video ad serving and management service. In conclusion, our research demonstrates that developing a blockchain video ad

server offers a promising solution to address the shortcomings of traditional ad-serving platforms.

[10] Bin et al. proposed in research on blockchain-based digital copyright protection began with digital copyright management and gradually transitioned to technology applications and breakthroughs. In brief, blockchain technology has enormous possibilities for digital copyright protection, but the development of digital copyright protection requires interdisciplinary collaboration and extensive research. It is necessary to improve user education on copyright protection awareness, balance the interests of authors and users, and accomplish complete digital copyright protection development. Blockchain, as a significant technological tool, should continue to be tested and verified in order to determine its practicality and usefulness in practical digital copyright protection scenarios. Theoretically, it expands knowledge of blockchain's possible application in digital copyright protection by emphasizing the novel effects of its primary characteristics—decentralization, immutability, and smart contracts—on ordinary copyright management.

[11] Koffka Khan et al. describe about comprehensive review of security in adaptive video streaming has provided a nuanced understanding of the multifaceted challenges and solutions within the dynamic landscape of multimedia content delivery. The examination of adaptive streaming architectures, protocols, and security mechanisms has revealed both the strengths and limitations inherent in current approaches. From vulnerabilities like content piracy and privacy concerns to potential attacks such as DDoS and man-in-the-middle, the security landscape is complex and continually evolving. The importance of ongoing research in addressing these evolving security challenges cannot be overstated. As the industry advances, so do the tactics employ by malicious actors. To stay ahead of emerging threats, continuous innovation and adaptation of security measures are essential. The integration of artificial intelligence, machine learning, and other emerging technologies presents promising avenues for enhancing the robustness and adaptability of security frameworks.
Limitation\Future Scope: The collaborative efforts of researchers, industry stakeholders, and policymakers will play a pivotal role in shaping a future where adaptive video streaming is not only seamless and adaptive but also secure and resilient against the evolving landscape of cyber threats. The journey towards secure adaptive video streaming is ongoing, and its successful navigation will undoubtedly contribute to a more trustworthy and user friendly digital environment.

[12] Koffka Khan et al. introduced the integration of blockchain technology into Content Delivery Networks (CDNs) for adaptive video streaming represents a significant paradigm shift with profound implications for the future of video streaming technologies. This exploration has highlighted the potential of blockchain to address key challenges in traditional CDNs, offering decentralized storage, transparent transactions through smart contracts, and enhanced security features. The implications extend beyond technical improvements to fundamentally alter the dynamics of content delivery, providing a more resilient, transparent, and user-centric streaming experience. The potential impact of integrating blockchain into CDNs for adaptive video streaming is far-reaching and holds the promise of shaping the future landscape of video streaming technologies.
Limitation\Future Scope: While challenges such as scalability and regulatory considerations need to be addressed, the future of video streaming technologies appears poised for a transformation that aligns with the principles of decentralization, transparency, and user empowerment that blockchain brings to the table.

[13] Koffka Khan et al. explores the transformative potential of blockchain in the realm of content authentication and copyright protection within the context of adaptive video streaming. The paper provides a comprehensive overview of adaptive streaming technologies, emphasizing the challenges associated with piracy and copyright infringement. It delves into the fundamentals of blockchain technology, discussing its decentralized, immutable, and transparent nature. The main focus lies in investigating how blockchain can be effectively leveraged to authenticate video content, employing cryptographic hashing, digital signatures, and smart contracts. Additionally, the paper examines blockchain's role in addressing piracy challenges through decentralized content distribution and verification mechanisms.
Limitation\Future Work - In essence, the recommendations for future research and practical implementations emphasize a holistic approach. Addressing technical challenges, environmental concerns, legal frameworks, user adoption, and fostering collaborative ecosystems will collectively contribute to

unlocking the full potential of blockchain in reshaping the landscape of adaptive video streaming, ensuring security, transparency, and equitable access in the digital media era.

[14] Koffka Khan et al. explain as the demand for high-quality video streaming experiences continue to rise, ensuring reliable and accountable Quality of Service (QoS) metrics becomes paramount. This review paper explores the transformative potential of blockchain technology in addressing the challenges associated with adaptive video streaming. By establishing a decentralized and tamper-resistant ledger, blockchain contributes to transparent QoS metrics, mitigating existing limitations in reliability and accountability. The conceptual framework involves the integration of blockchain principles, particularly smart contracts, to automate and enforce service level agreements. The paper delves into the advantages of blockchain, such as transparency, security, and tamper resistance, while addressing scalability issues and adoption challenges.

[15] Koffka Khan et al. explores the intersection of adaptive video streaming and network congestion models, aiming to provide a comprehensive understanding of how mathematical models can simulate and predict network congestion scenarios. author delve into the evolution of video streaming technologies, highlighting the challenges posed by fluctuating network conditions and the motivation for developing adaptive streaming algorithms. The core focus of this paper lies in elucidating various network congestion models, presenting an in-depth analysis of mathematical frameworks, parameters, and variables employed in these models. Additionally, author provide an overview of existing adaptive streaming algorithms and discuss their ability to dynamically adjust to network conditions. Limitation\Future Scope: Recognizing the limitations of traditional algorithms, author propose the integration of network congestion models as a solution to enhance adaptive streaming performance. Through the exploration of case studies and experiments, author validate the effectiveness of network congestion models in predicting and mitigating congestion scenarios. Finally, author discuss future research directions, suggesting avenues for advancing the integration of network congestion models with adaptive streaming. The paper concludes by emphasizing the importance of this interdisciplinary approach and its potential to shape the future of video streaming technologies.

## 3. METHODOLOGY

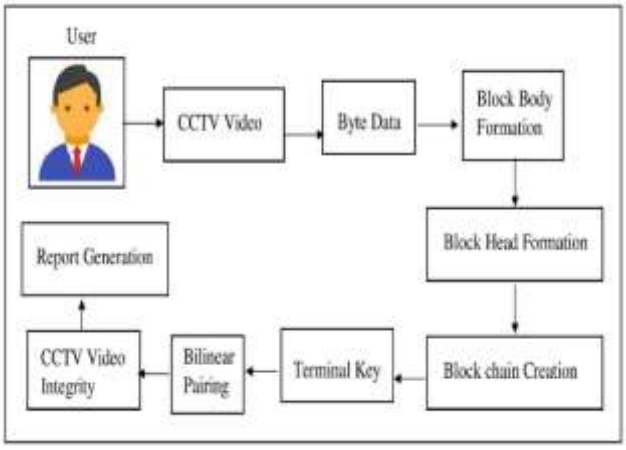


**Figure 13 System Overview**

The presented technique for the purpose of achieving securing CCTV through blockchain has been illustrated in the system overview shown in figure 1 above. The proposed approach has been attained through the implementation of a number of steps that are described below.

**Step 1:** CCTV Video Collection and Preprocessing – An interactive Graphical User Interface is developed using the Swings Framework of the Java Programming Language on the NetBeans Integrated Development Environment. This user interface is being used for the purpose of providing the CCTV video as an input to the system. The CCTV data is then read effectively and the Byte data is generated and provided for the next step for the purpose of Blockchain formation.

**Step 2:** Security through Blockchain– This phase makes use of the stored Byte Data achieved linearly through the previous step. Each of these CCTV videos are initiated with their own threads for the purpose of storing it securely.

Before the data is being stored, the byte data are being used for the purpose of implementing the blockchain framework. This is done through the calculation of the hash key for the byte data through the use of the MD5 bit hashing technique. The resultant hash key is then shortened through the use of random character selection to maintain a reasonable key length.

Eventually, the block chain's block head and block body are obtained. This procedure is being repeated for all of the byte data in order to obtain the final head key as the terminal key. These keys are stored and used in the next step for the purpose of integrity evaluation though Bilinear Pairing.

**Step 3:** Integrity Evaluation using Bilinear Pairing – The Blockchain for the CCTV byte data is created in the previous step through the hash key calculation. The terminal key is generated in the previous step is stored securely is then utilized for the integrity evaluation through the detection of an Avalanche effect.

The whole process of blockchain generation, as described in the previous phase, is repeated in the first layer of the Integrity examination. The received terminal key is therefore contrasted to the previously saved terminal key. If both terminal keys are exactly identical, the data can be considered secure; otherwise, the integrity review will proceed to the second layer.

The first layer of the Integrity assessment is depicted in equation 1.

$$\boldsymbol{f(BI)} = \int_0^n (PT! = CT) \Rightarrow f(NTE) \_\_ (1)$$

Where,

f(BI)=Block Integrity
N=Number of CCTV video
PT=Previous Terminal Key
CT=Current Terminal Key
f(NTE) =Next Tier Evaluation

Each newly formed CCTV video terminal key is matched to the CCTV video previously stored CCTV terminal keys in the second layer of the integrity assessment. Individual CCTV video are regarded private and protected if all of respective CCTV video terminal keys are equivalent to their corresponding prior keys. Conversely, any shard whose keys are not identical is considered to be compromised.

The previously stored head key of the compromised CCTV video is utilized as the previous key in the following shard to verify its integrity. Any alterations in the bit of the data blocks cause the resultant head key to have an Avalanche effect. This process continues until all of the CCTV video integrity findings have been recorded. Subsequently, the acquired findings are used to build a CCTV video Integrity Report that is displayed in an interactive User Interface, including the appropriate warning.

## 4. RESULT AND DISCUSSION

An effective strategy for detecting document integrity and conducting its analysis has been laid out in this research study. The approach has been really implemented using the Java programming language and the NetBeans IDE. This development system is outfitted with an Intel Core i5 CPU, 600 GB of storage, and 4 GB of RAM. Everything associated with storing databases has been handled by the MySQL Database server.

Detailed below is an account of the extensive experimentation that was conducted to evaluate the performance of the proposed methodology.

This module's performance enhancements can be successfully realized throughout the system.

The experimental setup will attempt to determine the time required to construct a blockchain as the number of documents increases. Table 1 below documents the findings of the module's performance evaluation.

| No. of Document | Block chain Creation Time | Key Generation Time |
|---|---|---|
| 10 | 4 | 2 |
| 20 | 16 | 13 |
| 30 | 32 | 34 |
| 40 | 44 | 50 |
| 50 | 52 | 58 |
| 60 | 64 | 61 |
| 70 | 69 | 71 |
| 80 | 77 | 73 |
| 90 | 81 | 79 |
| 100 | 95 | 97 |

**Table 1:** Blockchain creation and key generation time

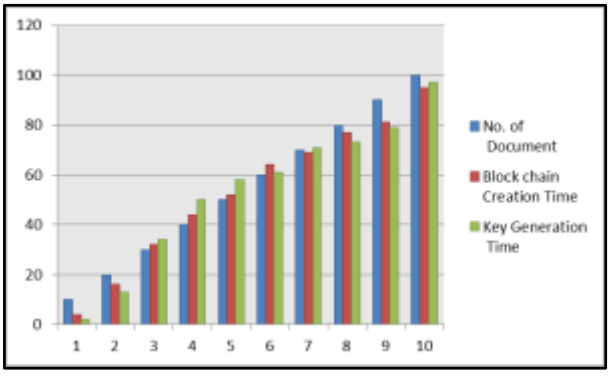


**Figure 2:** Blockchain & key generation Time

Figure 2 above shows a useful graph that uses the values gathered as the subsequent results. The experimental evaluation's findings show that the time needed to generate the blockchain and keys does not scale linearly with the rising document count. This indicates that the model is successfully implemented in its initial trial.

## 5. CONCLUSIONS

CCTV video Storage is one of the applications of blockchain. There are many ways to store it using blockchain. But what matters here is the size of the CCTV video. The data in the block can only be a string or anything which is in kilobytes. As the size of the CCTV video or files will be in megabytes, it is not logically correct to store the CCTV video directly in the blocks. Hence, the CCTV video can be stored in an off-chain storage system like the local machine or any distributed file system. In the present work, a blockchain network is created for storing the CCTV video. Incidents that allow the CCTV video to be falsified are also discovered owing to the unavailability of a competent storage medium. Despite the fact that security issues still exist, digital accreditation solutions have been used to solve this issue. One of the most existing technology that may be utilized for information security is blockchain. The block chain's inescapable nature aids in the prevention of CCTV video counterfeiting.

## REFERENCES

[1] Nikhil Bhusari, Tejaswini Kshirsagar, Akash Chandlekar, Apurva Borude, Kiran Gaikwad, “Efficient Model for Video Integrity through blockchain,” JETIR, May 2021, Volume 8, Issue 5, www.jetir.org (ISSN-2349-5162)

[2] A. Fitwi and Y. Chen, "Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain," 2021 International Conference on Computer Communications and Networks (ICCCN), Athens, Greece, 2021, pp. 1-8, doi: 10.1109/ICCCN52240.2021.9522199.

[3] Min-Hyuk Jeong and Sang-Kyun Kim, “Video Streaming Based on Blockchain State Channel with IoT Camera,” Journal of Web Engineering, Vol. 21 3, 661–676. doi: 10.13052/jwe1540-9589.2134.

[4] Eryk Schiller, Elfat Esati, Burkhard Stiller, “IoT-based Access Management Supported by AI and Blockchains,” University of Zurich University Library Strickhofstrasse 39, CH-8057, Zurich, DOI: https://doi.org/10.23919/CNSM52442.2021.9615523

[5] D. Na and S. Park, "Blockchain-Based Dashcam Video Management Method for Data Sharing and Integrity in V2V Network," in IEEE Access, vol. 10, pp. 3307-3319, 2022, doi:10.1109/ACCESS.2022.3140419.

[6] Moolikagedara, K.; Nguyen, M.; Yan, W.Q.; Li, X.J. Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. Electronics 2023, 12, 3621. https://doi.org/ 10.3390/electronics12173621

[7] Y. Ding, Z. Wu and L. Xie, "Enabling Manageable and Secure Hybrid P2P-CDN Video-on-Demand Streaming Services Through Coordinating Blockchain and Zero Knowledge," in IEEE MultiMedia, vol. 30, no. 1, pp. 36-51, 1 Jan.-March 2023, doi: 10.1109/MMUL.2022.3191680.

[8] Hira, F. A., Khalid, H., Ahmed, N., & Alam, M. M. (2023). User Acceptance of Blockchain Video Direct Observation Therapy mHealth App for Tuberculosis Patient Monitoring: A Pre-Implementation Phase Empirical Study. International Journal of Academic Research in Accounting Finance and Management Sciences, 13(2), 361–373.

[9] Sartzetakis Nektarios, Dermenoudis Konstantinos, Vafeias Michail, “VidAdChain: An innovative blockchain approach for digital video ad serving and management,” Int ernational Conference on Contemporary Marketing Issues, Corfu, Greece, 12-14 July 2023

[10] Bin, L., Yasin, M. A. I., & Rahman, S. N. A. (2023). Exploring Blockchain-Based Applications for Digital Copyright Protection. International Journal of Academic Research in Business and Social Sciences, 13(8), 1145 – 1157.

[11] Koffka Khan, “A Review of Security in Adaptive Video Streaming,” International Journal of

Multidisciplinary Research and Publications (IJMRAP), Volume 6, Issue 6, pp. 341-349, 2023.

[12] Koffka Khan, "Blockchain-Based Content Delivery Networks for Adaptive Video Streaming Optimization," International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 6, Issue 7, pp. 141-148, 2024.

[13] Koffka Khan, "Blockchain for Secure Adaptive Video Streaming: Addressing Copyright Protection and Anti-Piracy Challenges," International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 6, Issue 7, pp. 174-180, 2024.

[14] Khan, K. (2024). Blockchain-Driven Assurance: Transforming Adaptive Video Streaming with Tamper-Resistant Quality of Service Metrics. J Electrical Electron Eng, 3(3), 01-10.

[15] Koffka Khan and Wayne Goodridge, "Optimizing Adaptive Video Streaming: A Comprehensive Review of Network Congestion Models and Integration Strategies," International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 6, Issue 7, pp. 237 243, 2024.