International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 2, Mar-Apr 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Securing CCTV Video through Blockchain

R.S Kakade[1], Gite Anuja[2], Jadhavar Sakshi[3], Phopase Darshan[4], Sarode Prathamesh[5]

*1 HOD, Department of Computer Technology, Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology & Engineering(Polytechnic), Loni, Maharashtra, India

*2,3,4,5Department of Computer Technology, Padmashri Dr. Vitthalrao Vikhe Patil Institute of Technology & Engineering(Polytechnic), Loni, Maharashtra, India

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

Abstract:

From its humble beginnings as an immutable ledger of cryptocurrency transactions, blockchain technology has evolved into a dynamic platform for the development of trustworthy, decentralized apps. Despite the widespread usage of blockchain technology, no prior effort has focused on creating an immutable system for managing the provenance of scientific data that can automatically verify the records of provenance. Here at the office, we're using blockchain technology to help with the verification, management, and compilation of data provenance in an honest way. Incidents that enable the CCTV video to be fabricated also become apparent as a result of the absence of an effective storage mechanism. Despite the fact that security issues persist, CCTV video systems have been implemented to tackle this problem. One of the newest technologies that can be utilized for data protection is blockchain. The immutable nature of the blockchain provides a solution to the issue of CCTV video counterfeiting.

Keywords: **Blockchain, CCTV Video, Security.**

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

I. INTRODUCTION

The content of CCTV footage is sensitive and should not be easily accessible. Thus, a system that verifies the authenticity of the content in CCTV footage is highly necessary, since it is impossible to know for sure whether footage has originated from a reliable source or not. Furthermore, only authorized individuals should be able to access the confidential information contained in the paper. By utilizing blockchain technology, the likelihood of CCTV video forgeries may be reduced, and the security, authenticity, and privacy of CCTV footage can be improved. One example of a similar field technology is digital fingerprints, which are utilized in closed-circuit television footage for the purposes of authenticity, trustworthiness, and nonrepudiation. However, it fails to quickly commence the validation of the public key CCTV video status and has critical security gaps according to the specifications of a CCTV video. For instance, it uses the keys to authenticate the alteration of the record. If the key is compromised, this could lead to the acceptance of a forgery. There has been authentication of the signer's public key credential, but not of the signed document itself. Within the context of a CCTV Certificate, the signed document is likewise a CCTV video, which may or may not have a valid duration.

The authority presents the user with CCTV video that uses digital signature technology, which verifies the user's identity and grants them access to network resources. When it comes to traditional financial services, manufacturing, retail online purchases, public services, etc., CCTV video can be expanded to cover e-government activities and e-commerce on the internet. These sectors are interested in the use of identity verification and data protection. The era of blockchain technology is the bedrock upon which Bitcoin and other emerging crypto currencies rest. Many view decentralization as the primary benefit of blockchain technology. It can facilitate decentralized peer-to-peer (P2P)

transactions, as well as distributed system coordination and cooperation, free from centralized control and mutual belief among character nodes. This is achieved through the use of techniques like information encryption, time-stamping, distributed consensus algorithms, and monetary incentive mechanisms. The high operational costs, poor performance, and possible security threats of statistics garage in traditional centralized organizations have long plagued the industry, but blockchain technology has the potential to provide a novel alternative.

[1] This study work by Nikhil Bhusari et al. lays out the methods for a successful approach to integrity evaluation in detail. Videos have become an integral part of people's daily lives due to their great use and effectiveness. While most smartphones do come with high-tech camera sensors that can take decent films, the vast majority of those videos end up being used for spying purposes. In order to effectively and usefully incriminate a criminal, videos are utilized as evidence in legal proceedings. To achieve this goal, the system uses the video as an input and extracts frames from it. Using the RSA encryption technique, the video frames are effectively encrypted once they have been removed. The key generation module receives these encrypted frames and passes them on to it. You can develop a blockchain platform with the keys generated by this module, which are used to encrypt frames.
The next step is to formalize this strategy into an API so that it may be more easily integrated and evaluated in order to facilitate future research paths.

[2] in According to A. Fitwi et al., privacy and security are major concerns in the field of video monitoring. So, to share stored surveillance films securely and with privacy in mind, this study suggests SePriS, a private blockchain-based system that also includes an efficient video frame enciphering method. This exemplifies the potential of blockchain technology to address long-standing issues with surveillance practices, such as the misuse and leakage of stored videos. Video frame enciphering process passes typical computational and security standards, according to experimental study. Plus, they back up the suggested decentralized system's security, privacy, authenticity, controllability, auditability, and accountability when it comes to sharing stored surveillance videos. When it comes to video surveillance, the SePriS system strikes a nice mix between privacy and usability, which is the design goal.

[3] A scenario for the operation of an Internet of Things (IoT) camera video streaming system was proposed and put into place by Min-Hyuk Jeong et al. The DApp may connect to Internet of Things (IoT) cameras online and receive video streaming services independent of platform thanks to blockchain 2.0's standardized application programming interfaces and smart contracts. The author investigated off-chain transactions as a means to combat a low TPS and provide adequate compensation in the event of service mistakes. The author concluded that the state channel approach was the best off-chain transaction for the video streaming system of Internet of Things cameras after examining the three alternatives. By incorporating the state channel method into the video streaming system for IoT cameras, a novel scenario for the system was suggested.
Limitation\ Work to Come - Moving forward, we need to create a more intricate media service scenario that can accommodate many media items, including a speaker, a display, and a microphone, instead of just a basic smart contract camera for DApps.

Section 2 In this study provides a literature review of pertinent works; Section 3 Detail the methodology used in the study; Section 4 Analyzes the results of the experiments; and Section 5 ends by outlining potential areas for future research.

II. LITERATURE SURVEY

[4] A first-of-its-kind access management system that integrates AI, Blockchains (BC), and the Internet of Things (IoT) is described by Eryk Schiller

et al. Therefore, in order to access a resource, the user must pose for a camera. The system takes the image of that person and checks, whether this given user has the right to access a given resource. The internet-of-things gadget does the facial recognition and detection processing itself. A Multi-Task Cascaded Convolutional Network (MT-CNN) equipped with Mobile Nets (MN) was used for face detection. In addition, a Convolutional Neural Network (CNN) serves as the foundation for the Face Recognition model. Using the Hyper Ledger Fabric (HLF) to create immutable, tamper-resistant storage ensures a high degree of transparency by storing both the AI-decided access rights and the sensor-taken images.

[5] In order to guarantee the accuracy of Dash cam video data, D. Na et al. detail the current difficulties associated with blockchain technology, including the oracle problem and data privacy. A client for transmitting the transaction to the blockchain is chosen from among the nodes, and the vehicles connected to the V2V network are grouped according to GPS data; this solves the oracle problem. Each transaction is recorded in the blockchain by the client; scene data is stored in multiple images. It is also confirmed that the latency in the proposed structure does not significantly impact the overall system performance by measuring the performance of the proposed overall system. First, the study found that capacity increases when blockchains record multiple signatures. Second, vehicle IoT devices are unable to function as blockchain nodes. Third, GPS data reliability verification has its limits. Limitation\ In the Long Run: The author intends to investigate approaches to lightweight block chains that use block weight reduction methods, consensus algorithms, multi-signature compression, and RSU-based vehicle grouping in the future.

[6] The study's hypotheses are supported by Moolikagedara, K. et al.'s video blockchain framework. The results show that smart city surveillance systems with a video blockchain greatly enhance data integrity and security. According to this result, incorporating a video blockchain creates a strong security system for storing and retrieving video information from surveillance cameras. Video data is safeguarded from alteration and unauthorized access thanks to the integration of blockchain technology, third-party certification authority (CA) verification, and car cameras. Finally, the suggested video blockchain method improves the efficacy of surveillance systems in criminal situations by reducing the dangers of abusive attacks, data manipulation, and privacy breaches. This research makes a significant contribution by connecting blockchain technology with video frames recorded by smart surveillance systems. Vehicle camera video data transfers are now far more secure thanks to cryptographic mechanisms and decentralized storage platforms. The suggested blockchain-based method improves smart city trust, reliability, and controlled disclosure while simultaneously strengthening the security and integrity of vehicle video data. Limitation\ Down the Road: Despite these caveats, the authors intend to continue investigating ways to strengthen the system's defenses against quantum computer assaults in future projects. By enhancing the security and adaptability of an advanced vehicular distributed video network in smart urban environments, this solution is highly valuable for law enforcement monitoring, autonomous vehicles, insurance providers, and traffic control systems.

[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] Research has shown that there are several benefits for all parties involved when blockchain technology is integrated into video ad serving, as explained by Sartzetakis Nektarios et al. Ad impression verification and user verification can help advertisers become more transparent and trustworthy by guaranteeing that their content is being displayed to real people. Conversely, publishers stand to gain from better targeting capabilities and the abolition of ad fraud in terms of increased income possibilities. VidAdChain is a cutting-edge study that is currently developing a model for a system to manage and distribute video ads that are blockchain enabled. At this point in the research process, we have identified the primary obstacles to implementation and made headway in the algorithmic design of the system. At the moment, VidAdChain is working to resolve these obstacles and strives to showcase a functional prototype of a digital video ad serving and management service enabled by blockchain by the end of the project's term. Finally, our study shows that creating a blockchain video ad server is a great way to fix the problems with old-school ad servers.

[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] the eleventh 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 ofemerging 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\ In the Long Run: 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] A major paradigm change with far-reaching consequences for video streaming technology's

future has been introduced by Koffka Khan et al., who integrated blockchain technology into Content Delivery Networks (CDNs) for adaptive video streaming. Through its decentralized storage, transparent transactions enabled by smart contracts, and improved security features, blockchain has the ability to solve important problems with conventional CDNs, as our investigation has shown. Implications go beyond simple technological upgrades; they change the mechanics of content distribution from the ground up, making streaming more robust, transparent, and user-centric. The integration of blockchain technology into content delivery networks (CDNs) for adaptive video streaming could have a profound and far-reaching effect on the future of video streaming technology. Limitation\ Down the Road: Despite the fact that issues like scalability and regulatory concerns must be resolved, it seems like video streaming technologies are about to undergo a revolution that is in line with the decentralization, transparency, and user empowerment ideals that blockchain offers.

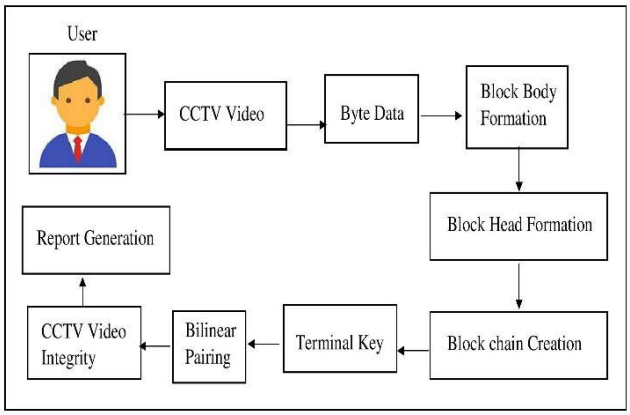
[13] In the context of adaptive video streaming, Koffka Khan et al. investigate how blockchain technology could revolutionize content authentication and copyright protection. Focusing on the difficulties caused by copyright infringement and piracy, the article gives a thorough review of adaptive streaming solutions. It explores the basics of blockchain technology, including how it is transparent, unchangeable, and decentralized. The primary objective is to investigate the most effective ways to utilize blockchain technology, such as cryptographic hashing, digital signatures, and smart contracts, for the purpose of authenticating video content. The essay also delves into blockchain's capabilities in addressing piracy issues by means of decentralized content distribution and verification methods. Limitation\ Looking Ahead: All things considered, the recommendations for further research and real-world applications demonstrate an all-encompassing strategy. Unlocking blockchain's full potential to reshape adaptive video streaming, ensure security, transparency, and equitable access in the digital media era will require addressing technical challenges, environmental concerns, legal frameworks, user adoption, and fostering collaborative ecosystems.

[14] Shubham gade et al. deployed the Hungarian model in his research which drastically reduces the time in allocating Ev changing vehicle slots. This allows the Hungarian neural network to handle slot

allocation in a more efficient manner. In order to assist in the resolution of the assignment problem, the Hungarian method that makes use of deep learning is referred to as the Hungarian Network (Hnet). Through the utilization of a deep learning neural network, this technique has the potential to be utilized for further deep learning problems that call for permutation invariant training (PIT). This Hungarian technique can be utilized can be used in the formation of the blockchain to maintain the smart contract process.

[15] Koffka Khan et al. explain as the demand for high-quality video streaming experiences continue to climb, establishing reliable and responsible Quality of Service (QoS) measurements becomes vital. This review paper investigates the revolutionary potential of blockchain technology in tackling the issues connected with adaptive video streaming. By building a decentralized and tamper-resistant record, blockchain helps to transparent QoS measures, addressing existing constraints in reliability and accountability.

METHODOLOGY



The method that has been suggested to establish a Securing CCTV Video through Blockchain system depicted in the system overview in Figure 1 up top.

The suggested method was based in part on the execution of the procedures detailed below.

Step 1: CCTV Video Collection and Preprocessing: The Java programming language's Swings Framework, in conjunction with the NetBeans IDE, is used to create an interactive GUI. The goal of this user interface is to provide the system with the CCTV footage. After that, the CCTV footage is properly deciphered, and the necessary byte data is produced and supplied to move forward with the Blockchain formation process.

Step 2: Security through Blockchain: The stored Byte Data obtained linearly in the previous stage is utilized in this phase. Separate threads are used to start each of these CCTV videos in order to save them safely.

Prior to storage, the byte data are utilized for the implementation of the blockchain framework. This is accomplished by utilizing the MD5 bit hashing algorithm to compute the hash key for the bytes of data. In order to keep the key length manageable, the generated hash key is then compressed using random character selection. The block head and block body of the block chain are eventually obtained. For each byte of data, this process is being iterated until the last head key is obtained and used as the terminal key. The following step involves storing these keys and using them to evaluate integrity using Bilinear Pairing.

Step 3: *Integrity Evaluation using Bilinear Pairing* : In the previous phase, the hash key calculation is used to generate the Blockchain for the CCTV byte data. Following its secure storage, the terminal key used for integrity verification in the previous step can be used to detect an Avalanche effect.

In this initial layer of the Integrity analysis, we replicate the entire blockchain generation process from the previous step. A comparison is thus made between the incoming terminal key and the one that was saved before. Data is considered secure if and only if the two terminal keys are identical; otherwise, the integrity check will move on to the second layer.

In equation 1, we can see the initial layer of the Integrity assessment.

$$f(BI)= \int 0\hat{}n((PT!=CT)\Rightarrow\top\ )\ f(NTE)\_ \ (1)$$

Where,

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

In the second tier of the integrity assessment, each key that is formed for the CCTV video terminal is compared to the keys that were previously stored for the CCTV video. All CCTV video terminal keys must be identical to their matching preceding keys for an individual CCTV video to be considered private and protected. On the flip side, keys that are different from one another indicate that a shard may have been compromised. To ensure its authenticity, the next shard uses the previously saved head key of the hacked CCTV footage as its previous key. The resulting head key experiences an Avalanche effect whenever the bit of the data blocks is altered. This procedure is repeated until every finding pertaining to the CCTV video integrity has been documented. After that, an interactive user interface displays a CCTV video Integrity Report that includes the relevant warning, based on the gathered findings.

III. RESULTS AND DISCUSSIONS

This research study has detailed the proposed methodology to enable an effective way for determining video integrity and its analysis. Using the NetBeans IDE and the Java programming language, the method has been realized. An Intel Core i5 processor, 600 GB of storage, and 4 GB of RAM make up the development machine's configuration. The MySQL Database server has taken care of all the duties related to database storage. The performance of the suggested methodology has been assessed through considerable experimentation, which is detailed in the part provided below.The whole system's performance can be effectively realized through the performance improvement in this module.

As the number of videos increases, the experimental setup will try to find the time it takes to form blockchain. The performance of the module is evaluated, and the results are documented in table 1 below.

No of Video	Blockchain Creation Time	Key Genration Time
10	3	2
20	15	13
30	31	32
40	46	52
50	51	54
60	61	58
70	65	68
80	74	71
90	76	73
100	96	98

Table 1: Blockchain creation and key generation time

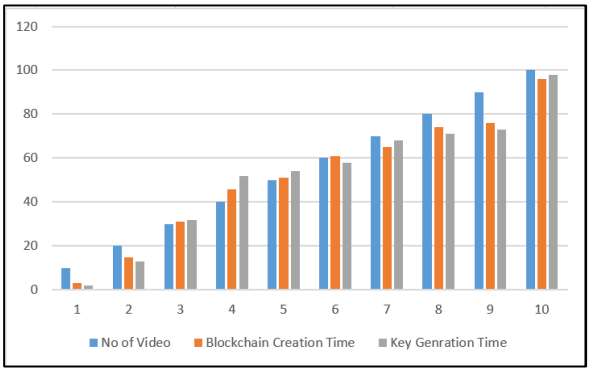


Figure 2: Blockchain & key generation Time

An effective graph is shown in figure 2 above using the values acquired as the subsequent outcomes. The results of the experimental evaluation make it clear that the time required to generate the block chain and keys are not directly proportional to the increasing number of videos. This represents the model is deployed properly in its first experiment.

IV. CONCLUSION AND FUTURE SCOPE

Storage of CCTV footage is one use case for blockchain technology. It can be stored in a variety of ways using blockchain technology. The quality of the CCTV footage is critical in this case. Any data stored in the block must be in kilobytes or be a string. Putting the CCTV footage straight into the blocks doesn't make sense because the file sizes will be in megabytes. Therefore, the CCTV footage can be saved in a distributed file system or an off-chain storage system, such as a local workstation. To store the CCTV footage, a blockchain network is built in this work. Because a reliable storage medium is not readily available, incidents that enable the falsification of the CCTV footage are also uncovered. Although there are still security vulnerabilities, digital accreditation methods have been implemented to address them. Blockchain is one of the newest technologies that could be used to protect sensitive data. The immutability of the blockchain helps to forestall the faking of CCTV footage.

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 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] Shubham Gade, Amita Singh, Shubham Sarote, " Efficient H-net model-based slot assignment solution to accelerate the EV charging station searching process ",ISSN: 2349-6002,Volume:11 ,Issue: 6,PageNo: 2590-2597

[15] Khan, K. (2024). Blockchain-Driven Assurance: Transforming Adaptive Video Streaming with Tamper-Resistant Quality of Service Metrics. J Electrical Electron Eng, 3(3), 01-1

