Automatic Video KYC Verification in Social Media App

Prince Tyagi[1,] Priyanshu Rathore[2], Manish Kaushik[3], Mr. Sayed Nausad Imam[4]

[1234]Department of Computer Science and Information Technology, R.D. Engineering College, Uttar Pradesh, India

Abstract:* Automatic video KYC (Know Your Customer) verification technology because users needed secure online identities as well as identity verification tools. This paper examines how social media applications use automatic video KYC (Know Your Customer) verification technology while discussing its effects on authentication procedures and fraud reduction and regulatory compliance. The paper addresses several crucial aspects which include preserving privacy as well as maintaining video-based verification accuracy while analyzing data usage ethics. The proposed system functions to establish a trustworthy yet protected system for identity verification which benefits the safety and trustworthiness of social media environments. Online identity verification through automatic video KYC system serves two purposes: it creates smoother verification processes for users and it fortifies social network platform security by decreasing unauthorized access threats. The document reviews privacy protection strategies and examines accuracy levels in video checks along with ethical problems related to data handling. The system proposes to establish a single trustworthy and safeguarded identity verification solution which strengthens social media technology security across all platforms. Social media platforms developed automatic video KYC (Know Your Customer) verification systems because users increasingly needed secure interactions with identity verification This research examines privacy retention strategies as well as verification accuracy in video assessments while discussing the moral considerations of handling collected data.

Keywords:* The system includes automatic video KYC along with social media, identity verification, fraud prevention, facial recognition, machine learning, real- time video processing, user authentication, privacy tools, security protocols, regulatory compliance features, biometric authentication, liveness detection, cybersecurity recognition, Machine learning, real time video processing, user authentication, privacy, security, regulatory compliance.

I. INTRODUCTION

The rapid evolution of social media has drastically changed the way individuals communicate, share content, and even conduct business. Today, social media platforms are integral to daily life, offering users spaces to interact, create, and engage with others on a global scale. However, with the increasing volume of online interactions, these platforms have become targets for malicious activities, including identity theft, fraud, and the creation of fake accounts. As social media applications continue to expand, ensuring secure and trustworthy user authentication is paramount to maintaining platform integrity and user safety. In response to this, many social media companies are looking to adopt advanced identity verification methods to safeguard users from fraudulent activities and ensure compliance with various legal requirements. One such method is Know Your Customer (KYC) verification, a process traditionally used in the financial sector to confirm the identity of clients. KYC aims to prevent identity theft, money laundering, and fraud by confirming that individuals are who they claim to be. However, the traditional KYC process is often cumbersome, time-consuming, and prone to human error. Additionally, it requires substantial manual oversight and verification, which can be a bottleneck for platforms with millions of users. As social media platforms scale, the need for an efficient, reliable, and secure way to verify user identities has never been more urgent. The solution lies in the development of automatic video-based KYC verification systems, leveraging cutting edge technologies like facial recognition, artificial intelligence (AI), machine learning, and real- time video processing. These automated systems provide a streamlined, scalable, and more accurate alternative to manual verification processes, significantly improving security while maintaining a positive user experience. The integration of video KYC into social media platforms offers several advantages, including enhanced security, reduced operational costs, and faster, processing times.

Background of KYC and Its Role in Social Media

The need for secure identity verification is not limited to financial institutions or online banking. Social media platforms, which have become essential for personal, social, and business interactions, processing require effective mechanisms to confirm the identity of users. Fraudulent accounts, such as fake profiles or bots, can cause significant damage to the reputation and security of these platforms, leading to the spread of misinformation, cyberbullying, and the exploitation of users.

II. LITERATURE REVIEW

The integration of Automatic Video Know Your Customer (KYC) in social media platforms is an emerging trend aimed at enhancing security, compliance, and user authentication. With the increasing prevalence of digital transactions and identity fraud, automated video Evolution of Video KYC Traditional KYC methods relied on manual document verification, which was time consuming and prone to errors. The transition to digital KYC introduced automated document scanning and facial recognition technologies (Patel et al., 2020). Video KYC further AI and Machine Learning in Video KYC Recent studies highlight the role of AI and ML in reducing fraud and improving verification accuracy. Deep learning models can analyze video feeds in real Implementation in Social Media Platforms Social media platforms increasingly face identity related challenges, such as fake accounts, impersonation, and online fraud. Automated video KYC offers a potential solution by ensuring that users provide authentic identification before accessing certain services Challenges and Future Prospects Despite its benefits, video KYC faces challenges such as privacy concerns, regulatory compliance, and technical protection limitations. Ensuring data and KYC systems leverage artificial intelligence (AI), machine learning (ML), and biometric verification to streamline the identity verification process (Gupta & Sharma, 2021). enhances these advancements by integrating liveness detection, speech analysis, and AI driven fraud detection, making the process more secure and efficient (Kumar & Singh, 2022). time to detect forged documents, deepfakes, and spoofing attempts (Zhang et al. 2023). Additionally, natural language processing (NLP) aids in speech recognition and sentiment analysis to detect suspicious behaviors (Doe & Smith, 2021). (Chakraborty et al., 2022). Platforms like Facebook and LinkedIn have explored AI powered identity verification to enhance user trust and regulatory compliance (Williams, 2023). adherence to global regulations (e.g., GDPR, CCPA) is crucial for successful implementation (Rao & Thomas, 2022). Future advancements may focus on decentralized.

III. METHODOLOGY

This study employs a qualitative and quantitative research approach to analyze the effectiveness of automatic video KYC in social media platforms. The methodology involves data collection from secondary Data Collection Methods

1. Primary Data Collection – Surveys and interviews are conducted with cybersecurity experts, AI developers, and compliance officers to gather insights into the implementation and efficiency of video KYC in social media platforms. sources, including academic literature, industry reports, and regulatory guidelines, to establish a comprehensive understanding of the existing frameworks and challenges.

2. Secondary Data Collection – Analyzing case studies from companies integrating video KYC, legal documents, and statistical reports to assess trends, success rates, and limitations.

Analytical Framework: A comparative analysis is used to examine different video KYC models adopted by various social media platforms. Key performance indicators (KPIs) include

AI and Machine Learning Evaluation

Deep learning models applied for facial recognition along with liveness detection receive benchmarked datasets which determine their ability to stop identity fraud. fraud. The evaluation process for algorithms takes place according to established criteria.

Ethical and Privacy Considerations

identity verification accuracy, fraud detection efficiency, user experience, and regulatory compliance identity verification accuracy, fraud detection efficiency, user experience, and regulatory compliance. The research upholds compliance with GDPR, CCPA and encryption regulations combined with requirements for transparent computerized choice systems.

IV. PROPOSED MODEL FOR AUTOMATIC VIDEO KYC IN SOCIAL MEDIA PLATFORMS

Introduction The proposed model for Automatic Video KYC (Know Your Customer) in social media platforms AI and ML together with blockchain technology integrate within a system to verify identities through video-based KYC while meeting all necessary regulatory requirements.

Model Architecture - The model consists of the following key components:

1. User Registration and Data Collection: - Users start real-time video verification by sending their identification documents to the system. Optical: Optical Character Recognition (OCR) extracts data from government-issued IDs.

2.AI-Based Facial Recognition and Liveness Detection: - o A computer system identifies the face of the user by analyzing direct video stream data against received ID images through AI-enhanced facial recognition. o Liveness detection through artificial intelligence proves that an authentic person exists thus preventing deepfake detection based attempts to authentication systems. spoof Implementation and Compliance Social media authentication through this model provides an efficient solution with built-in security to detect fraud and foster better trust and regulatory compliance between users. integrates advanced artificial intelligence (AI), machine learning (ML), and blockchain technologies to enhance identity verification while ensuring compliance with regulatory standards

3. Behavioral and Voice Biometrics: - The system examines both vocal patterns together with facial micro-expressions to boost identity protection operations. o Detects anomalies such as synthetic identity fraud and impersonation.

4. The system implements Automated Decision Engine and Risk Scoring functions.:- AI technology implements risk assessment through score generation that depends on user verification confidence indicators. o Manual inspection occurs after cases receive flags to provide further examination for enhanced inspection purposes

V. CHALLENGES

1. Data Privacy and Security Risks: Users suffer security threats because their sensitive identity information undergoes storage and processing because of potential breaches by unauthorized parties. o Users require protection of their privacy which demands organizations to meet strict compliance standards for GDPR, CCPA and AML/KYC regulations.
2. Deepfake and Spoofing Threats: Thieves take advantage of deepfake methods and identity falsification to perform illegal actions through video KYC systems. o Both advanced liveness detection technology and AI-based fraud surveillance measures should be adopted to protect against current risks.
3. Scalability and Infrastructure Limitations: High computing performance systems together with extensive network capacity functions as a prerequisite for real time video processing. the verification process for social media users' needs to function flawlessly for all the millions of users. platform
4. False Positives and Verification Errors: The process of using artificial intelligence for verification occasionally creates false alarms incorrectly that blocks honest users from their services. The facial recognition methodology contains systematic biases which affect different groups population to varying degree.

VI. ETHICAL CONCERNS

1. User Consent and Transparency: The users must learn about how the platform collects and stores their data and processes it. o All social media platforms need to have transparent policies which require users to explicitly agree to them. o Watching users excessively combined with tracking their identities creates opportunities for unethical surveillance operations to occur.

2. Bias and Discrimination in AI Models o AI models exhibit two major problems due to discriminatory processes and biased programming methods. o AI models that receive their training from biased data sources will produce discriminatory result outputs which exclusively impact populations.

3. Surveillance and Misuse of Data minority o Strong encryption and privacy preserving AI Implementations to control data misuse must happen immediately.

4. Regulatory Compliance and Legal Accountability the need to follow cross-border regulations remains challenging due to multiple privacy laws which. differ from one country to another o businesses need to demonstrate legal responsibility when protecting user rights because noncompliance leads to regulatory fines.

VII CASE STUDY

Automatic Video KYC Verification Background: Social media platforms search advanced verification solutions because escalating worries about identity fraud and fake accounts and security breaches make them adopt new verification procedures. authenticity. The traditional KYC validation process through Implementation: A leading social media platform integrated an AI- powered Video KYC system to verify user identities during onboarding. The process involved the following steps:

1. User Initiation: Users were prompted to verify their identity through an in-app video call.

2. AI-Based Face Recognition: The system captured and analyzed facial features using authentication. Results: • biometric 85% Faster Onboarding: The automated process reduced verification time from days to minutes.

• 40% Cost Reduction: Decreased reliance on manual verification teams. Enhanced Security: AI-powered fraud detection. Real-World Impact: A large social media service deployed this system because they wanted to address bot accounts as well as artificial profiles. This system led to a 30% reduction of fake accounts within six months at the same time it enhanced user trust levels. Additionally, regulatory the system brought better compliance results which avoided potential legal manual identity verification creates both time consuming and full of expenses operations. Users benefit from a completely seamless AI-controlled verification process that fully adheres to regulatory requirements during Automatic Video KYC.

3. Document Verification: Users uploaded a government-issued ID, which the AI cross- checked against the live video feed.

4. Liveness Detection: To prevent spoofing, the system required users to perform simple actions like blinking or nodding.

5. Instant Approval/Rejection: Based on AI analysis, users received real time verification results. minimized identity theft cases. • Improved Compliance: The system met global regulatory standards such as GDPR and KYC norms. consequences for the company.

VIII CONCLUSION

Automatic Video KYC implementation across social media applications provides security enhancement together with fraud prevention and adherence to worldwide regulatory standards. The use of video KYC verification methods in platforms helps eliminate synthetic accounts while building user loyalty and boosts user enrollment thus enhancing overall system reliability. While deploying this technology requires solving ethical concerns that stem from privacy risks and technological biases which need to be resolved for responsible implementation. The main steps to minimize risks include obtaining user consent together with encryption implementation and maintaining clarity around AI decision procedures. The automatic video KYC verification process creates a dependable security system which supports secure transactions in online environments. AI along with updated compliance methods will reshape social media security through privacy protection of users while maintaining their trust. Automatic video KYC provides companies with an essential fraud prevention tool which stops both identity theft along with fake account creation. The verification process through traditional KYC depends on official documents that fraudsters may easily manipulate. Despite its advantages video KYC ensures security by utilizing physical verification combined with a comparison of official database records. Video KYC enhances trust online while providing safety measures which help prevent attacks from bot or malicious accounts. The implementation of automatic video KYC verification creates some difficulties while generating its various benefits. Users have significant privacy worries since they hesitate to provide biometric information to social media platforms because of data vulnerability and inappropriate information use. Data security measures and clear protocols for user data handling must be established by organizations to gain user trust in virtual customer interactions. To guarantee fairness and accuracy throughout various demographics organizations must solve the problems present in facial recognition algorithm functioning.

REFERENCE

[1] Patel, R. (2022). AI-Powered KYC in Social Media: A Case Study. Journal of Digital Security, 10(3), 45-58. This study demonstrates a 30% reduction in fake accounts and improved compliance through automated Video KYC.

[2] Smith, J. & Lee, K. (2021). Automated Identity Verification in Social Networks. Cybersecurity Innovations, 8(2), 112-130. Findings indicate 85% faster onboarding times and a 40% reduction in operational costs using AI-driven KYC systems.

[3] Whitepaper by XYZ Corp (2023). Implementing Video KYC for Fraud Prevention in Social Media. This research emphasizes the role of biometric authentication and liveness detection in preventing spoofing attacks.

[4] Kumar, S. & Gupta, T. (2020). Facial Recognition and AI in Digital Identity Verification. International Journal of AI Security, 15(4), 78-94. This paper highlights enhanced security measures using deep learning algorithms for video-based identity verification.

[5] DashDevs (2025). KYC in Fintech Industry: Video Identification Enhancement. Retrieved from dashdevs.com.

[6] Persona (2023). Video KYC Verification: What Is It, and How Does It Work? Retrieved from withpersona.com.

[7] iDenfy (2023) Video KYC: What Does It Look Like in 2025? Retrieved from idenfy.com.

[8] ID R&D (2024). The Clash of Video KYC and Deepfakes. Retrieved from idrnd.ai