EVALUATIONZ

2024

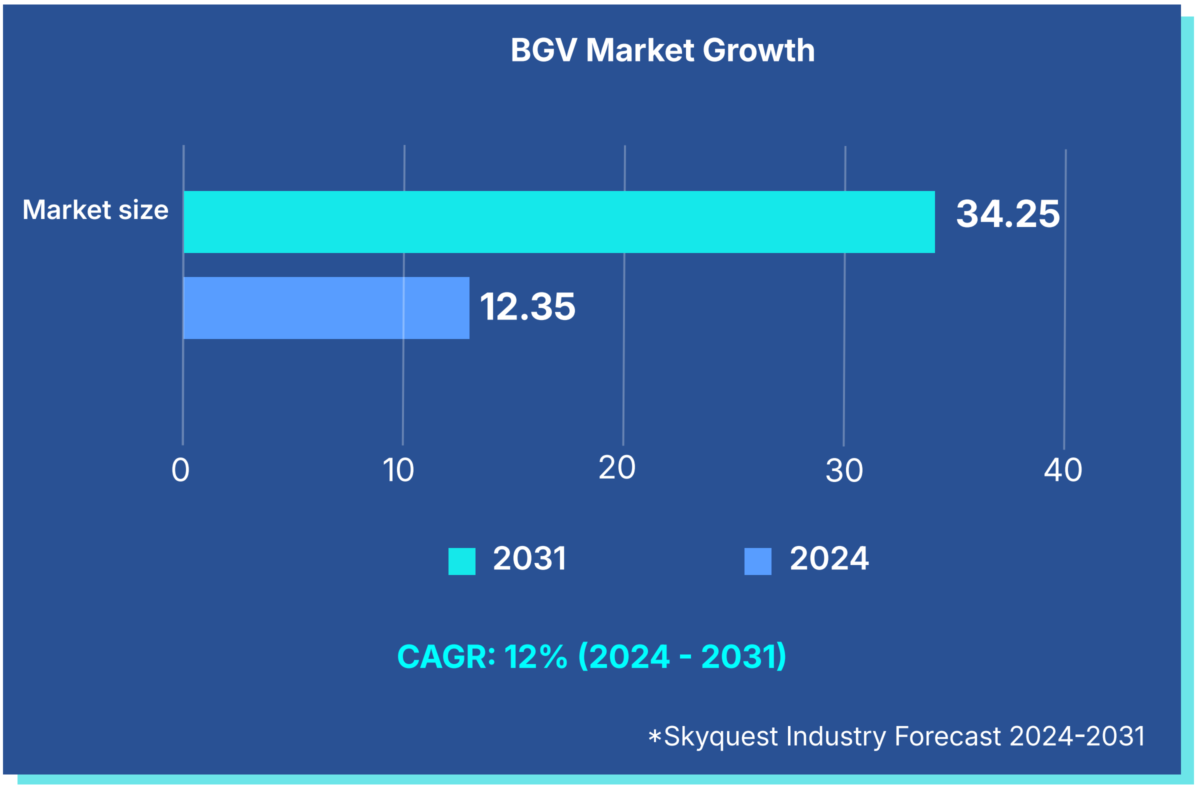
# Emerging Technologies in Verification and Their Impact on Businesses

# Introduction

As technology evolves, identity verification is becoming increasingly vital in various industries, from recruitment and financial transactions to healthcare and even online dating. The importance of verification lies in its ability to build trust, ensuring secure interactions and solidifying professional and financial relationships.

## Why Verification Matters

Verification serves as the foundation for trust in the digital world. It allows businesses to ensure they are dealing with legitimate users and customers, minimizing fraud and protecting sensitive information.



*Skyquest Industry Forecast 2024-2031

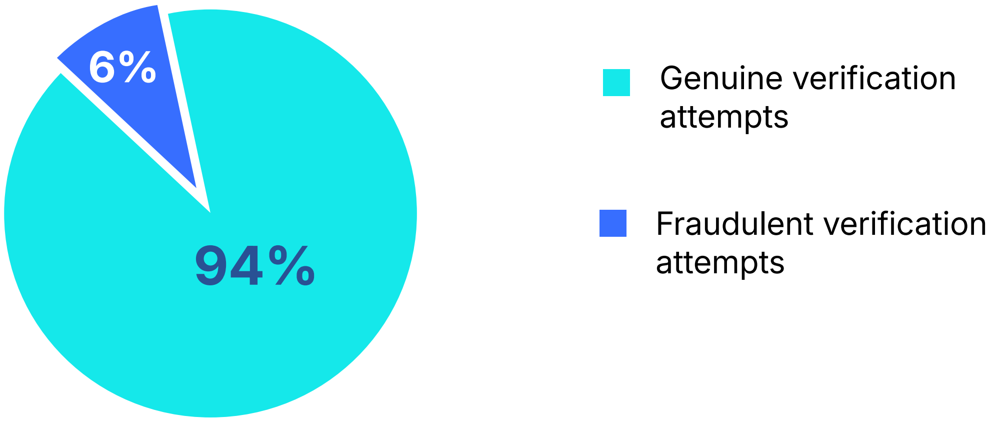
**12%**
**CAGR**

Globally, the background check market is experiencing significant growth. In 2022, it was valued at USD 12.35 billion and is expected to soar to USD 34.25 billion by 2031, with a Compound Annual Growth Rate (CAGR) of 12% from 2024 to 2031.

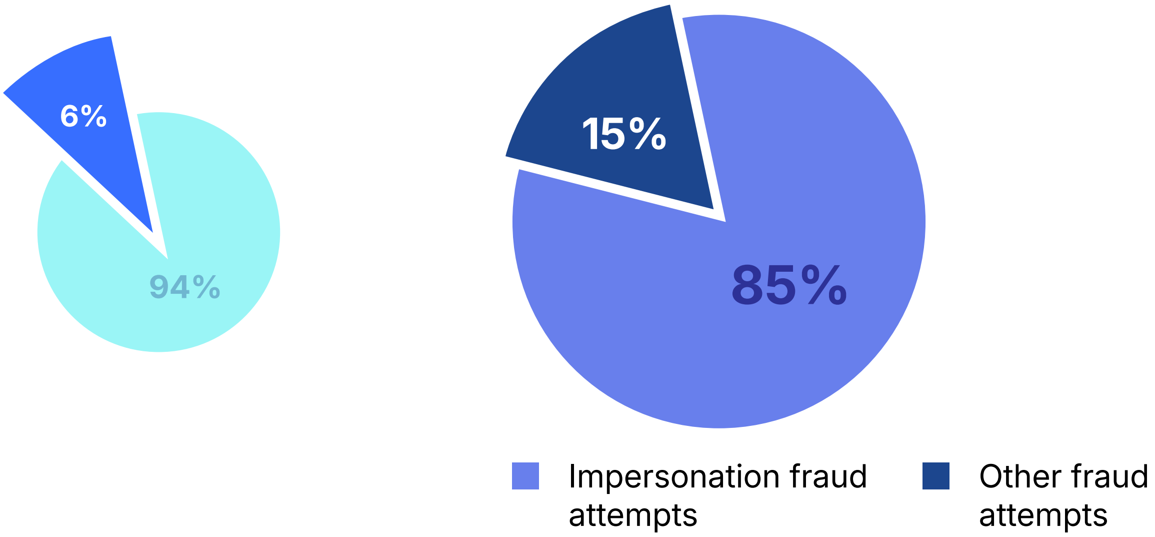
In an era where fraud and criminal activity are on the rise, more than 75% of consumers say they evaluate a company's fraud prevention record before doing business with them. Trust and security have never been more critical for businesses looking to thrive in the digital age.

**2023**

## % OF FRAUDULENT VERIFICATION ATTEMPTS



## BREAKDOWN OF FRADULENT VERIFICATION ATTEMPTS



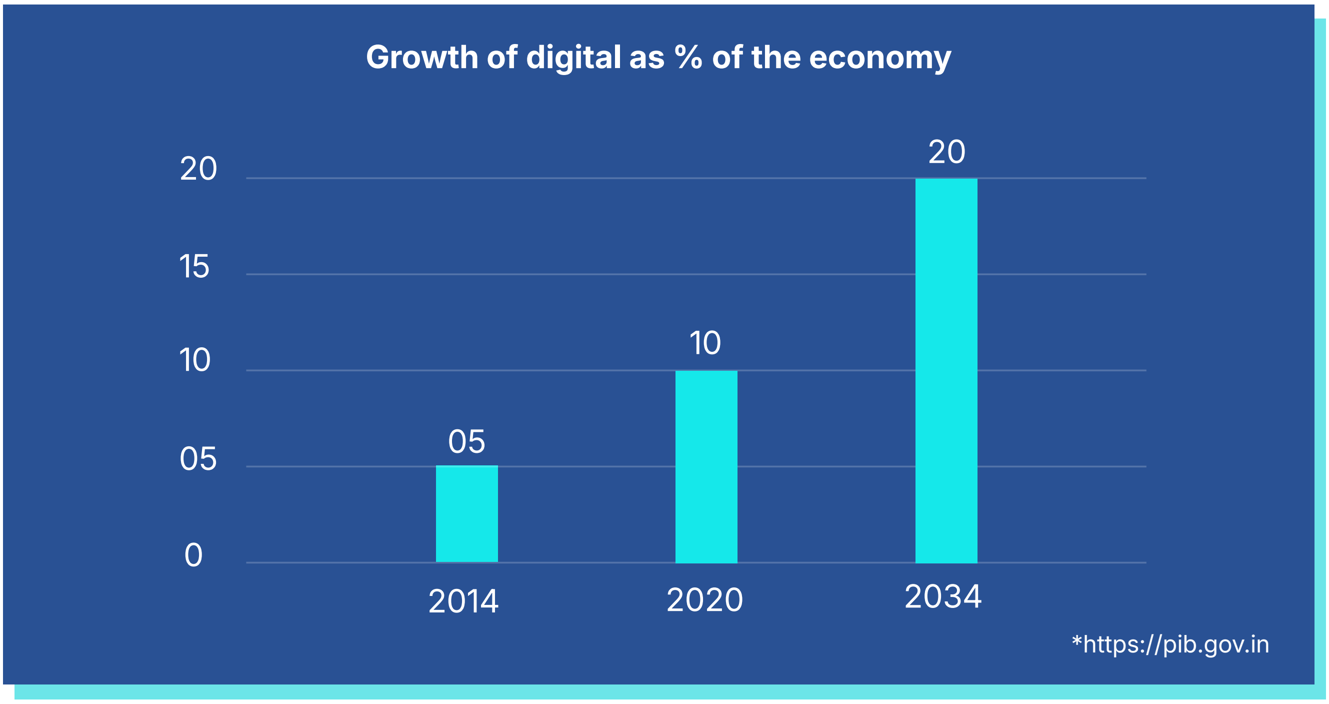
*Veriff Identity Fraud Report 2024

In 2023, 6% of all verification attempts were fraudulent, and identity fraud was the top concern. Of all fraudulent activities, 85% involved impersonation fraud.

# Increased Digitization in India

India is experiencing rapid digitization across sectors such as digital payments, governance, healthcare, and infrastructure. The BharatNet project is the government's ambitious ambition to connect every hamlet to high-speed internet and will contribute to overall growth across the country.

This presents both opportunities and challenges in fraud prevention. More digital services mean more avenues for fraudsters to exploit weak verification systems. Businesses must embrace cutting-edge technologies to stay ahead.

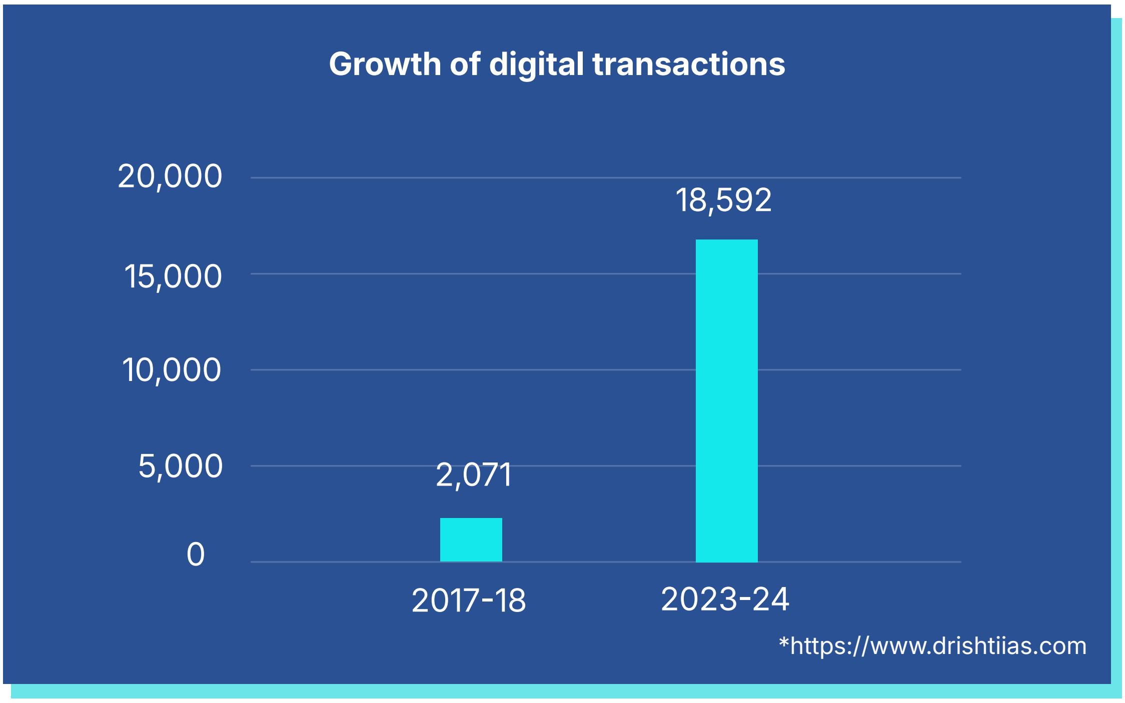


*https://pib.gov.in

The digital economy and its percentage of the total economy were 4.5 % in 2014 and 10% today in India. Experts believe that India's digital economy will reach 20% of the total economy by 2026

# Digital payments

The Unified Payments Interface (UPI) has transformed digital payments in India, with exponential development since its debut.



*https://www.drishtiias.com

In 2023-24, the total volume of digital payments in India was 18,592 crore, up 44% from 2,071 crore in 2017-18

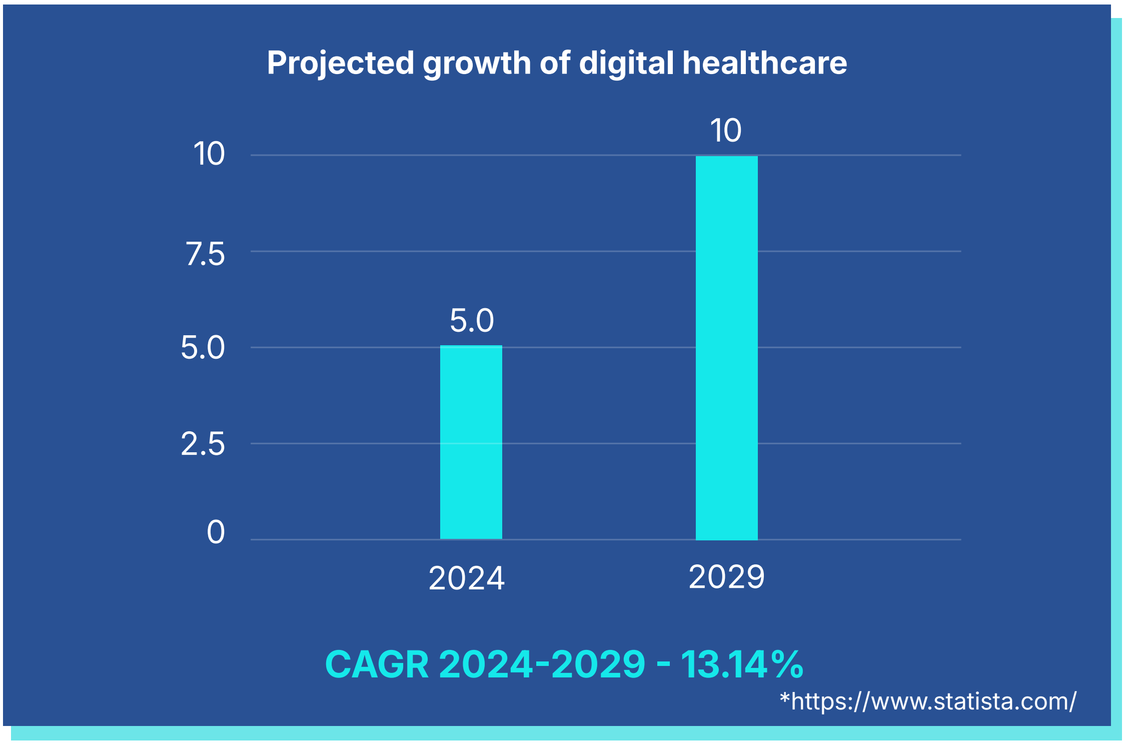
Total transaction value is estimated to grow at an annual rate of 11.56% (CAGR 2024-2028), with a projected total of US$394.40 billion by 2028

The market's largest market is Digital Commerce, with a projected total transaction value of US$211.30 billion in 2024

# Digital healthcare

The Ayushman Bharat Digital Mission serves as the centerpiece of India's digital health ecosystem. As of December 2023, 50 crore people have an Ayushman Bharat Health Account (ABHA) as their unique health identifier.

**50,00,00,000 people**



*https://www.statista.com/

Revenue in the Digital Health industry is expected to reach $5.34 billion by 2024. One major reason for its rise is that it makes medical care more accessible.

**$5.34 Billion**

**By 2024**

Revenue is estimated to grow at a 13.14% annual rate (CAGR 2024-2029), with a projected market volume of $9.90 billion by 2029.

**$9.90 Billion**

**By 2029**

# Digital governance

**19%**

**Over Apr 2022**

Aadhaar, India's biometric identification system, has become the foundation for numerous government and business sector services. In April 2023, Aadhaar holders completed over 2 billion authentication transactions, representing a 19% increase over April 2022.

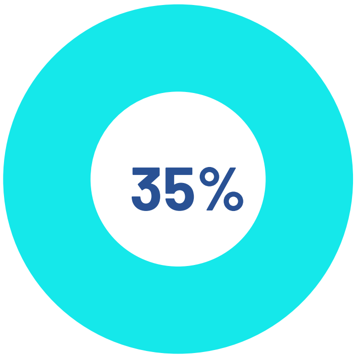
In addition, the government has undertaken a number of digitisation measures in the tax and compliance system. For example, the Goods and Services Tax Network (GSTN) enables firms to file tax returns electronically, making it easier to meet the criteria. Furthermore, the e-Way Bill system has helped track the movement of goods and verify compliance with the law.

# The Rise of New Fraud Techniques

As verification technology improves, so do the tactics used by fraudsters. New techniques like deepfakes, synthetic identities, and voice cloning present serious challenges for businesses.

## 1 Deepfakes

With deepfakes, AI technology is used to create fake video or audio recordings of individuals for the purpose of committing fraud. Over 35% of U.S. businesses have faced deepfake-related security incidents, with the use of AI to mimic voices and video becoming a growing concern.



**U.S. BUSINESSES DEEPFAKE SECURITY INCIDENTS**

## 2 Deepfake Voice frauds

37% of all businesses have experienced deepfake voice fraud,  Nearly half of all UAE (48%) and US (46%) businesses report experiencing this form of fraud. A notable incident in 2021 involved scammers cloning the voice of a company director, convincing bankers to authorize a $40 million fund transfer.

**$40,000,000**

*Regula Forensics

## 3 Video Deepfakes

40% of US businesses reporting they've experienced these, far above the global average of 29%. 28% of all small and medium-sized businesses  have experienced deepfake video fraud.

**40%**

*Regula Forensics

# Types of deepfakes

## Face swaps

When one person's face is superimposed not a video or photo of someone else, using perhaps Deep Neural Network or encoder technology. Some IDV tools could mistakenly approve the wrong person's identity

## Lip sync

These algorithms map a voice recording of the required audio content to a video if the person is saying something else which makes it appear that they are saying the words. This could be used to pass active liveness solutions or even human operator-based liveness solutions

## Puppets

A video records the desired movements of an actor, or the 'master'. It is overlaid onto a video of the target subject, with the 'puppet' then appearing to move like the master. This is difficult to detect and can defeat active liveness solutions.

## GANS & Autoencoders

GANs are trained on huge amounts of internet and social media data that show facial expressions and movements, then combined with an autoencoder to synthesise the facial movement of a digital version of a person. This can create fictitious yet convincing avatars.

## 4 Synthetic Identities

Synthetic identity fraud involves the creation of a new false identity using a mix of either real and false information, or a combination of real information from separate individuals. Because the identity is fictitious and leaves no identifiable consumer victim, it can be difficult for lenders and credit bureaus to detect and prevent synthetic identity fraud. In the USA, as many as 55% of businesses report that this has happened to them.

**55%**

**46%** of all small and medium-sized businesses  have already experienced synthetic identity fraud.

*Regula Forensics

## 5 Document Manipulation

When using this standard verification method, individuals submit identification, such as a passport or driver's license, which the company authenticates by comparing the document details with the information provided by the individual.

**13.7%**

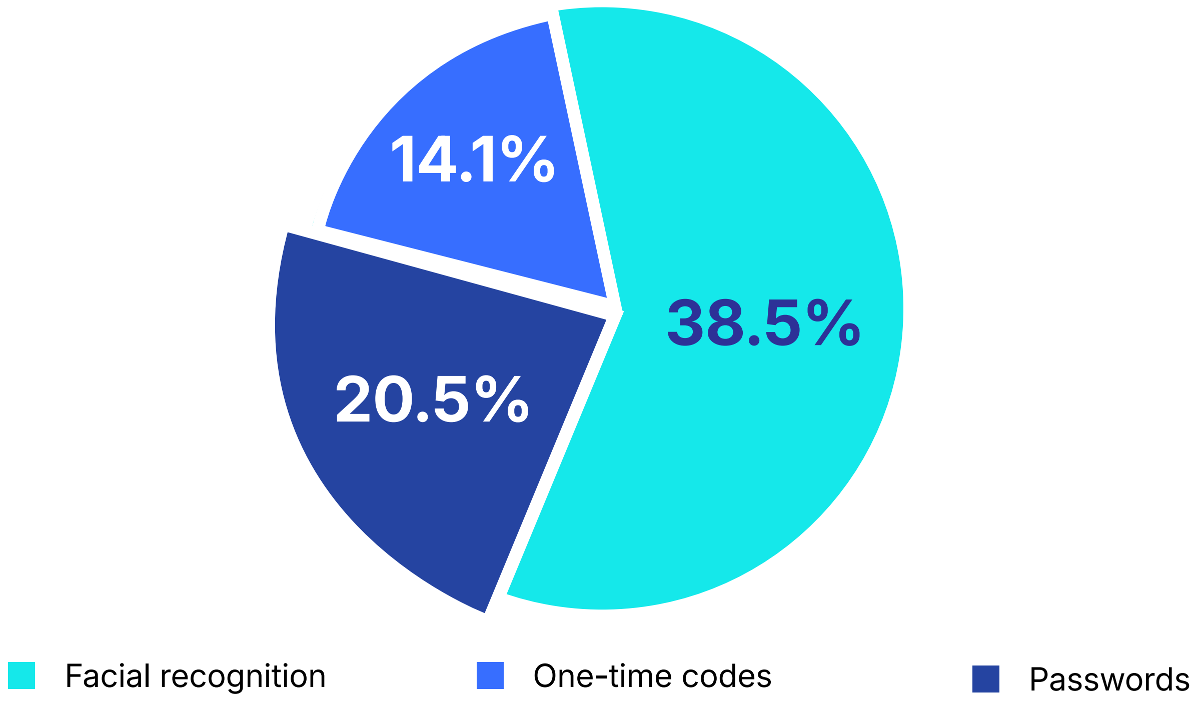
of fraud cases involved modified or fake documents

Impersonation fraud can manifest in different ways, such as starting the verification process with someone else's physical documents or synthetic IDs. In the past year, 13.7% of all fraud cases involved individuals presenting modified or fake documents.

# New Technologies and Their Impact

## 1. Biometric Advances

Moving beyond facial and fingerprint recognition, biometric technologies are gaining popularity. A recent survey shows that 38.5% of respondents see facial recognition as the most secure verification method, outpacing older methods like one-time codes (20.5%) and passwords (14.1%).



*Veriff Fraud Index 2024

Most respondents (60.5%) also expressed comfort with using facial recognition to access their accounts online; similarly, over half (51.6%) would be happy using IDs and selfies to confirm their identities

## 2. AI and Machine Learning

These tools are crucial for fraud detection and risk assessment. Machine learning models can adapt to new information, allowing businesses to stay ahead of emerging fraud techniques. However, AI is not a silver bullet; it must be combined with human oversight for more effective results.

## 3. Blockchain

As a decentralized and tamper-proof technology, blockchain can revolutionize identity verification by providing a transparent, immutable record of user identities.

## 4. Liveness Verification

This technique ensures that the individual undergoing verification is present in real-time, reducing the risk of fraud through static images or pre-recorded videos.

# The Future of Verification: A Human-Centric Approach

Despite the power of AI and advanced technology, human oversight remains crucial in identity verification. Humans are needed to guide AI, review cases flagged for potential fraud, and ensure that systems remain fair and unbiased. This "human in the loop" approach ensures that technology does not make crucial decisions without human input.

The verification landscape is evolving rapidly. Emerging technologies hold immense potential for creating a more secure and trustworthy digital environment. By staying informed about the latest advancements, businesses can utilize these powerful tools to protect themselves from fraud and enhance customer trust.

EVALUATIONZ