International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 12 | Dec 2025 www.irjet.net p-ISSN: 2395-0072

# Evolution of Technologies and their Relation to Scams and Frauds

**Anuj D Kankholi**

*Anuj D Kankholi(Student, MSc Cyber security), University Department of Information and Technology, University of Mumbai, Mumbai, India*

---

**Abstract:** *The rising use of ultramodern technologies has not only served society but also attracted fraudsters and culprits to misuse the technology for fiscal benefits. Fraud over the Internet has increased a lot, resulting in a periodic loss of billions of dollars and loss of service providers worldwide. Fraud directly impacts individualities, both in the case of cyber surfer-grounded and mobile-grounded Internet services, as well as when using traditional telephony services, either through landline phones or mobile phones. Druggies of the technology must be both informed of fraud, as well as defended from fraud through fraud discovery and forestallment systems. In this paper, we present the deconstruction of frauds for different consumer-facing technologies from three broad perspectives bandy Internet, mobile, and traditional telecommunication, from the perspectives of losses through frauds over the technology, fraud attack mechanisms, and systems used for detecting and precluding frauds.*

***Keywords: Cyber Frauds, Internet, Authentication Procedures, Analog technology, Repurpose digital, etc.***

## I. Introduction

The world as a whole has seen a rise in technologies in waves, some new trend or informative technology has always guided us forward. Although any or most of the technologies are made with the best intentions, Bad actors have always found a way to use those technologies to scam and fraud people. If we plot all the relevant technological advancements on a graph. The consumption of all relevant technologies has increased drastically. When new technologies emerged and people started using them, Bad actors and technological hackers got new ways into people's lives, and new ways to gather data. In the current world, Data is valuable.[1]

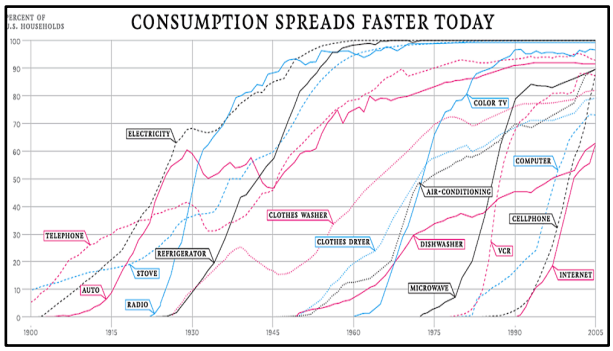


**Fig. 1.** Speed of Consumption of Technology [9]

Today, there are more than 1.5 billion such websites on the World Wide Web fewer than 200 million of them are working. The peak of 1 billion websites is hit for the first time in September of 2014. As per a survey of internet live stats, the overall number of sites has risen tremendously through 2016. The number of sites reached 900 million to 1.7 billion from January 2016 to December 2016 [12].

Scams and Fraud have existed for a long, and the availability of new ways to hack or gather data has only increased the frequency of scams and attacks.

This research paper seeks to delve into the intricate relationship between the evolution of technologies and the propagation of scams and frauds. By exploring how innovations in technology have both enabled and combated these illicit activities, we aim to provide a comprehensive understanding of this complex dynamic. As we venture through time and across the technological

landscape, we will examine the modus operandi of scams and frauds, the methods employed to perpetrate them, and the countermeasures designed to thwart their advances.

With an ever-present need to stay ahead of the curve in safeguarding against scams and frauds, this research paper aims to contribute to a deeper comprehension of the nexus between technology and deception. By shedding light on the historical and contemporary dimensions of this relationship, we can better equip ourselves and society at large to harness the potential of technology while safeguarding against its misuse. In doing so, we endeavour to provide a valuable resource for policymakers, law enforcement agencies, businesses, and individuals striving to navigate the evolving technological landscape with vigilance and resilience.

## II. LITERATURE REVIEW

The development of urban environments is increasingly being driven by knowledge-based approaches. Yigitcanlar argues that cities must evolve through the integration of human capital, knowledge infrastructure, and innovation systems to sustain economic and social growth in the 21st century [1]. Communication technologies have undergone major transformations. The telephone, as highlighted in a historical study, has significantly influenced both personal and professional interactions since its invention [2]. Similarly, the journey of radio from analog systems to digital platforms has been well documented, showcasing its enduring relevance in modern broadcasting [3].

The progression of computing technology has been marked by distinct generations, each bringing improvements in speed, architecture, and usability. This generational evolution, as discussed in [4], plays a crucial role in shaping today's digital systems and services.

Alongside these advancements, online fraud and cybersecurity threats have surged. A recent report by Ofcom highlights the growing frequency and complexity of digital scams, which target both individuals and organizations [5]. Real-world examples further underscore this issue: one individual lost ₹10 lakh in a bakery franchise fraud [7], and another was deceived through a screen-sharing app into transferring ₹17 lakh [8].

Artificial Intelligence (AI) continues to play a transformative role across industries. Saini explores how AI applications are being used for automation, decision-making, and pattern recognition, providing significant benefits in areas like healthcare and finance [6].

Technological innovation is now adopted faster than ever before. Gelman's analysis presents a timeline of how quickly new technologies reach widespread use, suggesting a consistent reduction in the time it takes for adoption curves to mature [9]. However, this acceleration has also contributed to an increase in tech-related scams. Nextiva reports a sharp rise in phone-based frauds, where scammers use tactics such as spoofing and impersonation to manipulate victims [10].

New-age tools like Flipper Zero demonstrate both the benefits and risks of advanced technology. As described in [11], this multifunctional device is marketed for educational purposes but can be used to interact with RFID, NFC, and other protocols—raising concerns over potential misuse.

The exponential growth of web-based content is another notable trend. Internet Live Stats provides data on the rising number of websites globally, reflecting the rapid digital expansion and its implications for access, regulation, and cybersecurity [12].

Ansar et al. conduct a comprehensive analysis of internet fraud cases, identifying common attack patterns and proposing countermeasures to improve online safety. Their research highlights the urgent need for technical and regulatory approaches to combat evolving threats in cyberspace [13].

## III. METHODOLOGY

The methodology section of this research paper outlines the approach used to conduct the study. It is important to note that this research is based solely on a comprehensive literature review and does not involve data collection or surveys. The aim of this methodology is to describe the sources, databases, and analytical methods employed to assess the evolution of technologies and their impact on scams and frauds.

1. **Literature Review** - The primary method employed in this research is an extensive review of the existing literature pertaining to the evolution of technologies and their correlation with scams and frauds. The following steps were taken to ensure a comprehensive and systematic literature review:

1.1. Search Strategy - A structured search strategy was developed to identify relevant literature. The search queries were formulated using a combination of keywords and Boolean operators to capture a broad spectrum of studies related to technology evolution and scams/frauds. Sample search terms included "technology evolution," "scams," "frauds," "cybersecurity," and "digital crime."

1.2. Inclusion and Exclusion Criteria - Articles and publications were included in the review if they met the following criteria: Relevance to the study's focus on technology evolution and its relation to scams and frauds. Publication in peer-reviewed journals or from reputable sources. Availability of full text for review. Articles were excluded if they did not meet these criteria or if they were not written in English.

1.3. Screening and Selection - The initial search results were screened based on title and abstract to assess their relevance to the research topic. Subsequently, selected articles were reviewed in full text, and relevant information was extracted.

2. **Data Analysis** - The analysis in this research is primarily qualitative, involving a critical examination of the literature collected. Key findings, trends, and insights from the reviewed literature were identified and synthesized to establish the evolution of technologies and their connection to scams and frauds. The analysis encompassed:

2.1. Identification of technological advancements over time.

2.2. Exploration of how these technologies have been exploited for fraudulent activities.

2.3. Examination of the countermeasures and solutions proposed in the literature to mitigate scams and frauds in the digital age.

3. **Ethical Considerations** - Since this research is solely based on the review of existing literature, no ethical concerns related to data collection, privacy, or human subjects were applicable.

This methodology section elucidates the process by which this research paper conducted a literature review to examine the evolution of technologies and their relationship with scams and frauds. By systematically searching, selecting, and analysing relevant literature, the study aims to provide a comprehensive understanding of this evolving landscape. The subsequent sections of the paper will present the findings and insights derived from this methodology, contributing to the broader discourse on technology-related scams and frauds.

## IV. ANATOMY OF SCAM

The anatomy of a scam and fraud typically involves several key components and steps that scammers use to deceive individuals or organizations for financial gain. While the specific tactics and methods can vary widely, here is a general overview of the anatomy of a scam and fraud:

1. **Identifying Targets**: Scammers often target individuals or entities based on various factors, such as their vulnerability, financial status, or personal information available in public records.

2. **Building Trust**: Scammers work to gain the trust of their targets. They might pose as a legitimate business, government agency, or a trusted individual. This can involve using official-looking logos, email addresses, or phone numbers.

3. **Creating a Story**: Scammers develop a convincing story or scenario to lure their victims. This story may involve promises of financial gain, urgency, or a threat to manipulate the victim's emotions.

4. **Initial Contact**: Scammers initiate contact through various means, including phone calls, emails, text messages, or even in-person meetings. They may use social engineering techniques to seem more convincing, such as pretending to be a bank representative or a family member in distress.

5. **Information Gathering**: Scammers may ask for personal information, financial details, or login credentials. They often claim that this information is necessary for a legitimate purpose, like verifying an account or providing a service.

6**. Urgency and Pressure**: Scammers often create a sense of urgency or pressure to rush the victim into making a decision. They might claim that the opportunity or the need is time-sensitive, leaving the victim with little time to think.

7. **Payment or Transfer**: To achieve their financial gain, scammers usually ask for money or assets. This can take the form of wire transfers, prepaid gift cards, cryptocurrency, or personal checks.

8. **Isolation and Secrecy**: Scammers may advise their victims to keep the transaction or communication secret. This prevents the victim from seeking advice or assistance from friends, family, or law enforcement.

9. **Obfuscation**: Scammers often use techniques to hide their true identity or location. They might use virtual private networks (VPNs), fake addresses, or disposable phone numbers to make it difficult to trace them.

10. **Disappearing Act**: Once they've obtained the victim's money or information, scammers typically disappear or cut off contact, making it challenging for victims to recover their losses.

11**. Repeat Offense**: In some cases, scammers may attempt to exploit the same victim multiple times or sell their information on the dark web, exposing them to further risks.

12. **Legal Implications**: Scammers often operate in violation of the law. If caught, they can face criminal charges and penalties.

Table 1: Fraud Cases in the Last 11 Fiscal Years

| Year | Cases | Amount (Crore) |
|---|---|---|
| 2018-2019 | 6,800 | 71,500 |
| 2017-2018 | 5,916 | 41,167.03 |
| 2016-2017 | 5,076 | 23,933.85 |
| 2015-2016 | 4,639 | 18,698.82 |
| 2014-2015 | 4,639 | 19,455.07 |
| 2013-2014 | 4,306 | 10,170.81 |
| 2012-2013 | 4,235 | 8,590.86 |
| 2011-2012 | 4,534 | 4,501.15 |
| 2010-2011 | 4,093 | 3,815.76 |
| 2009-2010 | 4,669 | 1,998.94 |
| 2008-2009 | 4,372 | 1,860.09 |

**Fig. 2.** Fraud Cases in Last 11 Fiscal Years [13]

## V. THE BEGINNING OF A TECHNOLOGICAL ERA WITH TELEPHONES

Invention Of The Telephone And Its Early Uses

Types Of Telephones and Ultramodern Uses Of Telephones

The electronic system was used for about a century, but in the 1960s, digital telephony came into play(Stefoff, 2005). Digital telephony was characterized by advanced quality and lower costs. It enabled people to communicate without paying attention to distances. [2]

Now, IP telephony is getting more and more popular. Governments, companies, and lots of people are using this type of telephony. At present, lots of people worldwide enjoy mobile phones that can penetrate every nanosecond. [2]

Scams conducted via telephone are unfortunately common, and they come in various forms. Here are some prevalent telephone scams:

1. Caller ID Spoofing: Scammers can manipulate their caller ID to display a trusted or legitimate organization's name or number, making it more likely that you'll answer the call.

2. Impersonating Government Agencies: Scammers might pretend to be from government agencies like the IRS, Social Security Administration, or even law enforcement, demanding personal information or payment to resolve fake issues.

3. Tech Support Scams: A scammer calls, claiming to be from a well-known tech company like Microsoft or Apple, and says your computer has a virus. They offer to help, gain remote access to your device, and often demand payment for their "services."

4. Fake Prize or Sweepstakes Calls: Scammers inform you that you've won a prize or lottery and ask for personal or financial information upfront, or they'll claim you need to pay taxes or fees to claim your winnings.

5. Debt Collection Scams: Scammers call, claiming you owe money and threaten legal action, arrest, or other consequences if you don't pay immediately. They may target individuals with actual debts or use fake debts.

6. Phishing Calls: Scammers pose as financial institutions or companies, asking for personal or financial information to "verify" your account details. They then use this information for identity theft or financial fraud.

7. Romance Scams: Scammers build a romantic relationship with victims over the phone, gaining their trust, and then requesting money for various reasons such as medical emergencies or travel expenses.

8. Charity Scams: Scammers impersonate charitable organizations, especially during natural disasters or holidays, to solicit donations. They often use high-pressure tactics to get you to give.

9. Loan Scams: Scammers offer fake loans with low interest rates and no credit checks, requiring an upfront fee. They disappear after you pay, and there is no loan.

10. Robocalls: Automated recorded messages that can be used for various scams, including offering fake services, making fraudulent investment offers, or demanding immediate payment for fictitious bills.

As we see the rise in the use of telephones the amount of scams has done through telephones also rises.

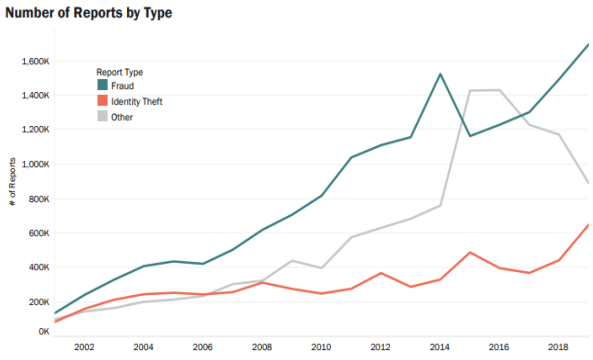


**Fig. 3.** Increase in the number of Scams by Phones [10]

Since 2002, we have seen an 800% increase in Fraud (Data collected from 2002 to 2018), and have seen 300% increase in Identity Theft (Data collected from 2002 to 2018)

## VI. INVENTION OF RADIO

Today, radios are a common technology found in homes, cars, and even on mobile phones. In fact, in today's society, it would be almost impossible to find anyone who has not used, seen, or heard of radio. However, this was not always the case because before the 19th Century, radio communication and transmission in its wireless form as we know it today was unheard of. Even after radio was developed in the late 1800s several years had passed before it became a household fixture. The history of radio is even more fascinating as it is filled with controversy; while Nikolai Tesla from Missouri, United States demonstrated the

workings of a wireless radio in 1893, credits go to Guglielmo Marconi as the radio's father and inventor. Marconi, of England, acquired this accreditation because he obtained the first wireless telegraphy patent in 1896. Eventually, Tesla acquired patents for basic radio in 1900. Still, in 1901, Marconi sealed the position of the first radio inventor by becoming the first individual to transmit radio signals across the Atlantic Ocean (Tech Wholesale, 2014). Before World War I, institutions mainly used radio to contact ships, which sailed out of sea. Radio communication at the time was particularly beneficial during emergencies.

During World War I, the usefulness of radio became significantly apparent as the military used it as a tool for receiving and sending messages to the armed forces. Following World War I, radio's use and popularity spread to include civilians with broadcasting stations cropping up in Europe and the U.S. Therefore, broadcasting stations such as British Broadcasting Company (BBC), Westinghouse's KDKA, AT&T, CBS, and NBC were created and each were offered specific rights such as toll broadcasting, chain broadcasting, manufacturing of transmitters, and manufacturing of receivers.

Today, the original radio broadcasting signals as invented by Tesla or Marconi have changed drastically. Traditional radio transmissions have evolved with the invention of Internet radio stations and satellite radio. Nowadays radios are found in homes, in vehicles, and other mobile devices. Additionally, the audience can now choose to listen to news, music, or talk shows.[3]

### Technologies that use Radiofrequency

Radiofrequency (RF) technology is a broad field that encompasses various technologies and applications. Here are some of the types of technologies and applications that use radio frequency:

1. Radio Broadcasting: Traditional AM (Amplitude Modulation) and FM (Frequency Modulation) radio broadcasting use RF to transmit audio signals over the airwaves.
2. Television Broadcasting: TV broadcasts use RF to transmit video and audio signals to television sets.
3. Wireless Communication: This includes technologies like:
    a. Cellular Networks: Mobile phones and smartphones communicate via RF signals with cell towers.
    b. Wi-Fi: Wireless routers and devices use RF signals to provide local area network (LAN) connectivity.
    c. Bluetooth: This short-range wireless technology is used in devices like wireless headphones, keyboards, and speakers.
    d. NFC (Near Field Communication): NFC enables proximity communication for applications like contactless payments.
    e. RFID (Radio-Frequency Identification): RFID is used for tracking and identifying objects and animals, often in logistics and inventory management.
4. Satellite Communication: RF signals are used to transmit data to and from satellites in orbit, enabling services like satellite television, global positioning (GPS), and satellite internet.
5. Radar Systems: Radar systems use RF waves to detect the range, speed, and other characteristics of objects. They are used in aviation, weather forecasting, and military applications.
6. Wireless Sensor Networks: These networks use RF to enable communication between various sensors and devices in applications such as industrial automation, environmental monitoring, and home automation.
7. Amateur Radio: HAM radio operators use RF technology for hobbyist communication and emergency services.
8. Microwave Communication: RF signals in the microwave range are used for long-distance point-to-point communication, often in the form of microwave links.
9. Remote Controls: Many remote controls for TVs, stereos, and other devices use RF technology.
10. Smart Grids: RF technology is used in smart grids to enable two-way communication between utility providers and smart meters in homes and businesses.
11. Radio Frequency Heating: RF is used in industrial processes to heat and dry materials like food and wood.

12. Avionics: RF technology is crucial in various aviation communication and navigation systems.
13. Security Systems: RF technology is used in security systems, including alarm systems and access control.
14. Healthcare: RF is used in medical devices, such as RFID-based patient tracking systems and some types of medical imaging.
15. Wireless Charging: Some wireless charging technologies, like Qi wireless charging, use RF signals to transmit power to compatible devices.
16. Military and Defence: RF technology is employed in various military applications, including communication, radar, electronic warfare, and surveillance.
17. Space Exploration: RF communication is used for data transmission from spacecraft and rovers to Earth.

### *Scams done using Radio Technologies*

Scams using radio technologies are relatively less common compared to phone or internet-based scams, but they do exist. Radio-based scams typically involve manipulating radio signals for fraudulent purposes. Here are some examples:

1. Pirate Radio Scams: Individuals or groups may operate illegal "pirate" radio stations to promote fake products, services, or events. They might advertise non-existent businesses or events, collect money for advertising, and then disappear.
2. Jamming Communications: Scammers with the equipment to jam radio frequencies can interfere with legitimate radio communications. For
example, they might jam the signals of emergency services, air traffic control, or law enforcement, creating a dangerous situation.
3. Rogue Broadcasting: Some scammers may gain access to or hack into legitimate radio stations to broadcast false emergency alerts or fake news. This can cause panic and confusion in affected communities.
4. RFID Scams: Radio-frequency identification (RFID) technology is used in various sectors, including retail and transportation. Scammers can use RFID skimming devices to steal data from RFID cards, such as credit cards or access cards, without direct contact.
5. Unauthorized Eavesdropping: Scammers with the right equipment can intercept and eavesdrop on radio signals. This can be used to gather sensitive information, such as conversations or data being transmitted over radio waves.
6. Impersonating Emergency Services: Scammers may impersonate emergency services on radio frequencies, spreading false information about emergencies or disasters. This can lead to unnecessary panic and confusion.

## VII. COMPUTER AND THE INTERNET

The history of computers dates back to the period of the scientific revolution (i.e. 1543 – 1678). The calculating machine constructed by Blaise Pascal in 1642 and that of Gottfried Leibnitz marked the birth of the operation of machines in assiduity.

This progressed up to the period 1760 – 1830 which was the period of the artificial revolution in Great Britain where the use of machines for products altered the British society and the Western world. During this period Joseph Jacquard constructed the weaving impend (a machine used in cloth assiduity).

In 1980 Microsoft Disk Operating System (MS-Dos) was born and in 1981 IBM introduced the particular computer for home and office use. Three times later Apple gave us the Macintosh computer with its icon-driven interface and the 90s gave us the Windows operating system. As a result of the colorful advancements in the development of the computer, we've seen the computer being used in all areas of life. It's a veritably useful tool that will continue to witness new development as time passes.[4]

The invention of the Internet is a complex and ongoing process that involves the development of various technologies and protocols over several decades. It is not attributed to a single inventor or a specific date. However, one significant milestone in the creation of the Internet is the development of ARPANET (Advanced Research Projects Agency Network), which can be considered the precursor to the modern Internet.

ARPANET was funded by the U.S. Department of Defense's Advanced Research Projects Agency (ARPA, later renamed DARPA) and became operational in 1969. It connected computers at four research institutions: UCLA, Stanford Research Institute, UC Santa Barbara, and the University of Utah. This network allowed researchers to share information and resources among the connected computers.

The development of ARPANET was a key step in the evolution of the Internet, but it took many years of research, experimentation, and the creation of various networking protocols to transform it into the global and interconnected network we know today. The internet has evolved through the contributions of numerous individuals and organizations over the years.

**Scams done using the Internet**

Scams conducted on the internet are unfortunately widespread, and they come in many forms. Here are some common types of internet scams:

1. Phishing Scams: Phishing involves sending fraudulent emails or messages that appear to be from legitimate organizations, such as banks, social media platforms, or government agencies. These messages often request personal information like usernames, passwords, or credit card details.

2. Advance Fee Fraud: Scammers promise a large sum of money, a job, or some other benefit in exchange for a small upfront payment. Once the payment is made, the promised benefit never materializes.

3. Online Shopping Scams: Fraudulent online retailers offer products at extremely low prices to entice shoppers. However, once a payment is made, the goods are never delivered, or the items received are of low quality.

4. Auction and Marketplace Fraud: Scammers on online marketplaces like eBay or Craigslist may post fake listings for goods or services, and then request payment but never deliver the items.

5. Romance Scams: Scammers create fake online personas to develop romantic relationships with individuals, gaining their trust before asking for money due to supposed emergencies, travel expenses, or other fabricated reasons.

6. Tech Support Scams: A scammer may claim to be from a well-known tech company, informing you of a computer virus or issue. They then gain remote access to your computer and demand payment for "fixing" the problem.

7. Investment and Ponzi Schemes: Scammers promise high returns on investments in various schemes or cryptocurrencies, but they are running Ponzi schemes where early investors are paid with funds from newer investors.

8. Social Engineering Scams: Scammers manipulate people into revealing confidential information through tactics like impersonating friends or family, posing as coworkers, or conducting fake surveys.

9. Ransomware Attacks: Malicious software is used to encrypt a victim's files or data, and a ransom is demanded in exchange for the decryption key.

10. Work-from-Home Scams: Scammers offer remote job opportunities that seem too good to be true, and they may require upfront fees for training, equipment, or materials that are never provided.

11. Email Account Compromise: Scammers gain access to an individual's email account and use it to send fraudulent emails or reset passwords on other online accounts.

12. Lottery and Prize Scams: Scammers inform victims that they've won a lottery or prize, but they must pay fees or taxes upfront to claim their winnings.

Nearly nine in ten adult internet users (87%) have encountered content online which they believed to be a scam or fraud. Nearly half (46%) of adult internet users reported having personally been drawn into engaging in an online scam or fraud, while four in ten (39%) reported knowing someone who has fallen victim to an online scam or fraud.

Overall Top Ten Scams

| | Scam Type | % of Total | Median Loss |
|---|---|---|---|
| 1 | Prizes/Sweepstakes/Free Gifts | 35.23% | $795 |
| 2 | Internet: Gen Merchandise | 19.58% | $500 |
| 3 | Phishing/Spoofing | 17.49% | $800 |
| 4 | Fake Check Scams | 5.59% | $2,000 |
| 5 | Friendship & Sweetheart Swindles | 3.35% | $925 |
| 6 | Investments: Other (incl. cryptocurrency scams) | 3.05% | $1,750 |
| 7 | Advance Fee Loans, Credit Arrangers | 2.31% | $700 |
| 8 | Family/Friend Imposters | 1.89% | $775 |
| 9 | Computers: Equipment/Software* | 1.05% | $1,100 |
| 10 | Scholarships/Grants | 1.02% | $1,000 |

**Fig. 4.** Recent Types of Scams over the Internet. [5]

On average, in the top 10 scams done on the internet, a person will lose between 500$ to 2000$.

## VIII. THE BLEEDING EDGE OF SCAMS AND AI

Artificial Intelligence (AI) is the branch of computer science that deals with the intelligence of machines where an intelligent agent is a system that takes actions that maximize its chances of success. It is the study of ideas that enable computers to do the things that make people seem intelligent. The central principles of AI include such as reasoning, knowledge, planning, learning, communication, perception, and the ability to move and manipulate objects. It is the science and engineering of making intelligent machines, especially intelligent computer programs. [6]

### Scams Done using Artificial Intelligence

Scammers are increasingly using AI (Artificial Intelligence) and machine learning techniques to enhance the sophistication and efficiency of their scams. While not an exhaustive list, here are some examples of scams involving AI:

Deepfake Scams: Deepfake technology uses AI to create realistic-looking videos or audio recordings that manipulate a person's image or voice. Scammers can use deepfakes to impersonate individuals and request fraudulent payments or share false information.

AI-Enhanced Phishing: Scammers use AI to craft highly convincing phishing emails or messages. AI can analyze the recipient's online activity and preferences, making the phishing content more targeted and persuasive.

Chatbot Scams: Some scammers deploy AI-driven chatbots that impersonate customer service representatives, sales agents, or even romantic partners. These chatbots engage with victims and lead them into scams or gather personal information.

Voice Synthesis Scams: AI can be used to generate synthetic voices that mimic real people. Scammers may use this technology for voice phishing, where they impersonate trusted individuals to request sensitive information or payments.

AI-Generated Fake News and Social Media Posts: AI can be used to create fake news articles, social media posts, and reviews. Scammers can spread false information to manipulate markets, damage reputations, or promote fraudulent products.

Automated Trading Scams: AI can be used in high-frequency trading or algorithmic trading schemes that manipulate financial markets for the scammer's benefit. These schemes can cause significant financial losses for unsuspecting investors.

Credential-Stuffing Attacks: AI-driven bots can automate the process of testing stolen username and password combinations on various websites, exploiting the fact that many people reuse passwords across multiple accounts.

Data Privacy Violations: AI can be used to analyze vast amounts of data for targeted advertising or other purposes, raising concerns about privacy violations. Personal data collected by AI systems can be exploited or sold without the individual's consent.

AI-Powered Email Attacks: AI can be used to generate convincing emails that impersonate trusted contacts or use social engineering techniques to deceive recipients into taking harmful actions, like wiring money or downloading malware.

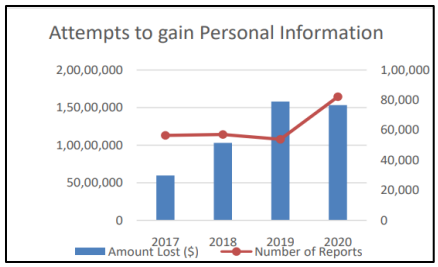


**Fig. 6.** Annual Report of Financial Loss with number of reports [13]

## IX. SOME MODERN-DAY SCAMS ARE DONE USING MODERN TECHNOLOGY.

1. Pune man loses Rs 10 lakh to online bakery chain franchise scam. Earlier in the year, several other complaints were recorded by the Pune police which had a similar modus operandi. An officer of the Cyber Crime police station said, "Franchise frauds have been reported from across India where names of notable brands are used to lure people into investing in new franchises and large sums are taken from them. People should be extremely careful while choosing the platforms through which these communications take place. People should cross-check these investment offers with the contact details given on the official websites of these companies." [7]

**2. A Gurgaon man cheated of Rs 17.5 lakh through a screen-sharing app.**

A Gurgaon man has alleged he was cheated of Rs 17.5 lakh by a man who posed as a customer care representative of a phone company. "A person introducing himself as an Airtel customer care representative with the name 'Manish' offered to help with the issue. I spoke with him a few times and he explained how to get a refund from Airtel. On June 4, he asked me to download an Android app named 'Anydesk' on my mobile phone," he said in his complaint. The police said the case was filed after a preliminary probe on the receipt of the complaint. The case is under investigation, they said. [8]

**Flipper-Zero: A case of good technology in bad possession.**

**Fig 5.** Flipper Zero: An Educational Device [11]

The Flipper Zero is a versatile programmable multi-tool device equipped with various hardware components tailored for security research and hacking purposes. Its hardware includes built-in modules for RFID/NFC communication, infrared signals, and radio frequency transmission and reception, making it capable of interacting with and manipulating a wide range of electronic systems and devices. Additionally, it features a programmable logic controller (PLC) that enables users to perform physical security assessments. The device's open-source nature and the ability to upload custom firmware make it highly adaptable for different applications and user needs while serving as an educational platform for learning about hardware hacking and security research.

**Types of attacks that can be done using Flipper Zero**

RFID/NFC Attacks: The Flipper Zero can clone or emulate RFID and NFC cards, allowing for unauthorized access to secure areas or systems.

Infrared Attacks: It can transmit and replay infrared signals to control and manipulate various IR-controlled devices, such as TVs, air conditioners, or remote controls.

Radio Frequency Attacks: The device can interact with and manipulate radio frequency communication, which may include analyzing and exploiting vulnerabilities in wireless communication systems.

Physical Security Assessments: With its programmable logic controller (PLC), it can be used to assess and manipulate physical security systems, such as access control, door locks, and alarms.

Penetration Testing: The Flipper Zero can be used as a tool during penetration testing exercises to discover vulnerabilities in computer networks, web applications, and other digital systems.

Reverse Engineering: Security researchers can use the device to reverse engineer hardware and software components, dissect and understand how certain systems work, and discover potential weaknesses.

## X. CONCLUSION

The rapid advancement of emerging technologies has revolutionized nearly every aspect of modern life, bringing unprecedented convenience, connectivity, and innovation. However, as our world becomes increasingly interconnected through the digital realm, it has also provided fertile ground for malicious actors to exploit these technologies for scams and fraudulent activities. This research paper has explored the intricate relationship between emerging technologies and the proliferation of scams, shedding light on the various ways in which these technologies are harnessed for nefarious purposes.

Our investigation revealed a complex and evolving landscape where scams constantly adapt to capitalize on the latest technological trends. From phishing schemes and deepfake manipulation to AI-driven fraud and cryptocurrency-related scams, the spectrum of deceptive activities has expanded dramatically. Scammers leverage these technologies to not only reach a broader audience but also to create more convincing deceptions, making it increasingly difficult for individuals to discern between genuine and fraudulent interactions.

Furthermore, this research underscores the far-reaching consequences of technology-enabled scams, affecting not only individual victims but also industries, governments, and society as a whole. Financial losses, data breaches, identity theft, and the erosion of public trust are some of the notable impacts that underscore the urgency of addressing this issue.

As our study has shown, combating the use of emerging technologies in scams demands a multi-pronged approach. Law enforcement agencies, regulatory bodies, and the technology industry must collaborate to develop robust cybersecurity measures and regulations that can adapt to the evolving nature of scams. Public awareness and education campaigns are also pivotal to empowering individuals with the knowledge and tools needed to protect themselves from falling victim to these scams.

In conclusion, the coexistence of emerging technologies and scams presents both challenges and opportunities. While the ingenuity of malicious actors continues to evolve, the same technologies can be harnessed to develop innovative solutions for prevention and mitigation. As we move forward, the key to effectively addressing this issue lies in our ability to stay ahead of scammers, adapt to the changing landscape, and harness the transformative power of technology for the betterment of society while safeguarding against its misuse. Only through continued research, collaboration, and vigilance can we hope to strike a balance that allows emerging technologies to fulfil their vast potential while minimizing their use in scams.

## References

[1] Yigitcanlar, T. Position paper: Redefining knowledge-based urban development. Int. J. Knowl.-Based Dev. 2011, 2, 340–356

[2] IvyPanda. (2022, August 16). Technologies: History of Telephone. https://ivypanda.com/essays/technologies-history-of-telephone/

[3] Kuyucu, Mihalis. (2019). The History Evolution of Radio in The World on its Digital Journey. ISBN- 978-9940-540-70-8

[4] Zakari, Ishaq & Yar, Umaru. (2019). History of computer and its generations.

[5] Executive Summary Report: Online Scams & Fraud Research https://www.ofcom.org.uk/__data/assets/pdf_file/0025/255409/online-scams-and-fraud-summary-report.pdf

[6] Prof. Neha Saini, Research paper on Artificial Intelligence and its Applications | ISSN: 2456-3315

[7] https://indianexpress.com/article/cities/pune/pune-man-rs-10-lakh-online-bakery-chain-franchise-scam-8968560/

[8] https://indianexpress.com/article/cities/delhi/gurgaon-man-cheated-rs-17-lakh-through-screen-sharing-app-8829424/

[9] https://statmodeling.stat.columbia.edu/2012/04/08/technology-speedup-graph/ - Speed of Consumption of Technology

[10] https://www.nextiva.com/blog/common-phone-scams.html - Increase in number of Scams by Phones

[11] Unlocking the Power of Flipper Zero: The Educational Tool Which Has A Multitude of Features Which Could Change Your Lives! - https://medium.com/@rshar272k/unlocking-the-power-of-flipper-zero-the-educational-tool-which-has-a-multitude-of-features-which-9b3c2548c11b

[12] Online Available at: https://www.internetlivestats.com/total-number-of-websites/

[13] Ansar, Syed & Yadav, Jaya & Dwivedi, Sujit & Pandey, Ankur & Srivastava, Savarni & Ishrat, Mohammad & Khan, Waris & Pandey, Dhirendra & Khan, Prof. Raees & Khan (2021). A Critical Analysis of Fraud Cases on the Internet. Turkish Journal of Computer and Mathematics Education (TURCOMAT)