CYBER FORGERY: AN ANALYSIS

Nikita Aggarwal, Amity Law School, Amity University, Mohali, Punjab

ABSTRACT

Cyber forgery is a growing form of cybercrime that exploits digital technologies to manipulate electronic records, documents, and identities with fraudulent intent. With the increasing reliance on digital platforms for communication, commerce, and governance, incidents of cyber forgery have become more frequent and sophisticated. This research paper provides an in-depth analysis of cyber forgery by examining its various types, underlying causes, and the techniques employed by offenders, including digital document alteration, identity impersonation, phishing, malware, and the misuse of artificial intelligence technologies such as deepfakes.

The study further explores the legal framework governing cyber forgery, highlighting relevant statutory provisions, judicial interpretations, and enforcement challenges. Through the analysis of notable case studies and real-life examples, the paper illustrates the practical implications and societal impact of cyber forgery. Additionally, the research discusses preventive measures, including technological safeguards, digital forensic tools, legal reforms, and user awareness initiatives aimed at mitigating cyber forgery risks. The paper emphasises the need for a multidisciplinary approach combining legal, technical, and educational strategies to effectively address the evolving threat of cyber forgery in the digital age.

1. Introduction

Cyber forgery has emerged as a critical challenge in the digital era, where criminals manipulate, fabricate, or alter electronic information for financial gain, deception, or malicious intent. This paper examines the diverse forms of cyber forgery, including identity theft, phishing, online signature forgery, credit card and banking fraud, document and certificate manipulation, and social media impersonation. It highlights the causes of these crimes, ranging from weak passwords and human negligence to malware exploitation, software loopholes, and the misuse of emerging technologies like artificial intelligence and deepfakes. Cyber forgeries manipulate, alter, or create digital information to deceive, gain an illegal advantage, or harm people, organisations, or governments. This allows fabrication of multimedia files, electronic signatures, scanning certificates, identification proofs, banking credentials, and even paper documents. The rapid growth of e-governance, online banking, e-commerce, and remote work has made cyberspace important to daily life. It has also given thieves additional opportunities to exploit system, human, and regulatory vulnerabilities. Cyber forging must be studied in the digital age to understand cybercriminals' strategies and their social, economic, and legal effects. Forged emails, fake websites, altered bills, fake academic certificates, and cloned social media profiles can damage reputations, confidence, finances, and digital transactions. Fraudulent documents, while hiring or purchasing or counterfeit credentials, allow illegal access to sensitive data, harm companies. Even governments struggle to stop sophisticated forgeries from compromising official correspondence, public records, and identity databases. This research will cover cyber forgery's primary types, offenders' strategies, and why systems and people are vulnerable. Reviewing Indian and foreign laws and case studies will highlight the issue's gravity and the need for strong legal deterrents. Awareness campaigns, organisational regulations, and law-enforcement-technology provider cooperation will complete the preventative measures. Security measures include digital signatures, encryption, and two-factor authentication. The report recommends enhancing detection and response systems to protect the benefits of digitisation from fraudulently manipulating electronic information. The paper explains the phenomena, impacts, and remedies to make digital technology safer and more trustworthy.

2. Literature review

2.1 Books and Academic Literature

A thorough literature review on cybercrime, information security, and computer forensics laid the framework for the theory. These materials helped us understand cyber forging, how it started, and where it fits in with digital crimes.

2.2 Research Papers and Scholarly Articles

Peer-reviewed literature from IEEE Xplore, Springer, ScienceDirect, and Google Scholar was analysed. This investigation examined current trends, advanced forgery detection tools, and prevention strategies. Papers from the recent five years were preferred for correctness and relevance.

2.3 Government and Law-Enforcement Reports

Global and national government reports provided credible facts and policy recommendations. CERT-In, MeitY, Interpol, and UNODC papers on legal frameworks, cyber-incident handling, and coordinated forgery responses were helpful.

2.4 Authentic Websites and Technical Portals

We researched digital signatures, encryption standards, and fraud prevention on cybersecurity, technology, and global watchdog websites. These portals included advisories, threat alerts, and technical white papers on online identity and document protection.

2.5 Case Reports and News Articles

Actual cyber forgeries were examined using case reports, investigative journalism, and trustworthy news sources. Fake e-mails, certificates, and banking data can affect individuals, corporations, and governments, as well as investigative agencies' efforts to find culprits.

2.6 Approach to Data Compilation

To ensure clarity and prevent plagiarism, all information was examined, compared, and summarised in the original language. To respect others' labour and maintain classroom honesty, we will cite our sources in the references.

3. Types of Cyber Forgery

Cyber forging occurs when criminals alter or create digital information to deceive, steal, or

gain illegal advantages. Form depends on target, medium, and method. Cyber forgeries in today's digital world fall into the following types.

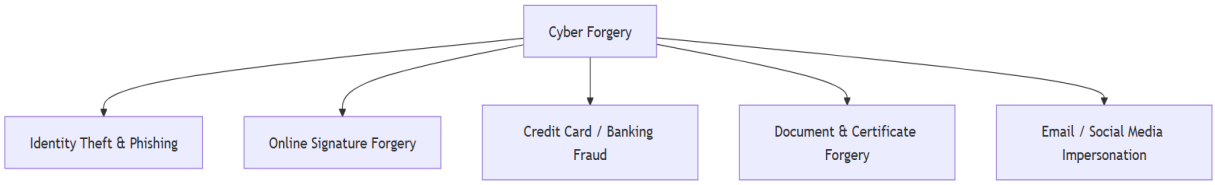

Figure 1: Types of Cyber Forgery (Wang et al., 2022)

3.1 Identity Theft and Phishing

Identity theft is a major global cybercrime. Identity thieves steal victims' names, addresses, login credentials, financial information, Aadhaar or Social Security numbers, and more. Phishing—sending fake emails, pop-ups, or texts as legitimate institutions—is a common approach. Responding to these messages may lead to unwanted financial transfers, malware installation, or password exposure. Cybercriminals sent around 1,500 Indian bank customers phishing emails posing as Reserve Bank notifications in 2022.[1] After clicking on fraudulent links, victims' credentials were stolen, resulting in several lakh rupees in unauthorised transactions. Smishing and vishing employ text messages and phone calls, whereas spear-phishing leverages public personal data to send personalised messages. If stolen identities are used in unlawful operations, the consequences go beyond money. Legal concerns, mental distress, and reputational damage are also possible. Users should use two-factor authentication (2FA), update their passwords often, avoid clicking on unexpected links, and verify the sender before answering. Banks and businesses mitigate risk with email screening, fraud detection algorithms, and awareness programs.

3.2 Online Signature Forgery

Electronic and scanned signatures in business and legal transactions increase the risk of online signature fraud. Digital signatures from images or scanned documents can be used to fake

[1] G. Wang, C. Wang, M. Shahidehpour, W. Lin. Deep semi-supervised learning method for false data detection against forgery and concealing of faults in cyber-physical power systems. IEEE Trans Smart Grid. 2.023;1.5(1):9.44-5.8

contracts, checks, and letter.[2] Hacking user accounts or altering digital certificates are advanced authentication bypasses. Fake authorisation letters to transfer funds from a worldwide firm's account in 2021 caused a company quarrel. Advanced software mimicked pressure and stroke patterns to digitally replicate signatures. Due to unexpected permissions, internal audits discovered the embezzlement. Forged signatures can cause legal issues, financial losses, contract breaches, and corporate governance disputes. These incidents threaten regulatory fines and confidence damage for institutions. Any credible organisation should use secure digital signatures, encryption, time stamping, and frequent data audits. Staff should learn to examine signatures and not rely on scanned materials.

3.3 Credit Card and Banking Fraud

Credit card and debit card cloning, fake banking instructions, and online banking vulnerability attacks are frequent financial sector cyber forgeries. Phishing, malware browser extensions, and skimming devices can steal bank data.[3] Scammers utilise business email compromise (BEC) methods to get employees to deposit money into bogus accounts. A 2020 BEC example involved a European corporation sending over $1 million to an offshore account using fraudulent invoices from a trusted supplier.[4] The study found that deepfake video interactions and email spoofing authorised the transactions. Due to these crimes, billions are lost annually. Others may suffer reputational damage and long legal proceedings to recoup payments. To reduce risks, use SSL encryption, tokenise credit card data, use multi-factor authentication, and monitor transactions. Employees must also learn to spot phishing communications and false payment instructions.

3.4 Document and Certificate Forgery

Fake diplomas, land titles, property deeds, medical records, and passports are possible with digital technology. Fraudsters may alter scanned copies, use complex graphic design tools, or create new templates to appear real. In 2019, a nationwide academic fraud ring selling fake degrees to online job seekers was busted. Some employees used bogus credentials before the

[2] K. Zarzycki, P. Chaber, K. Cabaj, ■awry■czuk M, P. Marusak, R. Nebeluk, et al. Forgery cyber-attack supported by LSTM neural network: an experimental case study. Sensors. 2.023;2.3(1.5):6.778.
[3] A. Sedik, Y. Maleh, El Banby GM, Khalaf AA, Abd El-Samie FE, Gupta BB, et al. AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities. Technol Forecast Soc Change. 2.022;1.77:121.555.
[4] Y. Wang, C. Peng, D. Liu, N. Wang, X. Gao. Forgerynir: deep face forgery and detection in near-infrared scenario. IEEE Trans Inf Forensics Secur. 2.022;1.7:5.00-1.5.

scam was discovered. Forged documents can cause illegal work, visa problems, insurance fraud, and ownership concerns. Physical verification institutions may struggle, and victims may face lengthy administrative and legal issues. Cryptographic certificates, blockchain-based verification, and QR codes are increasingly used by governments and organisations to verify authenticity. Businesses must employ secure online verification.

3.5 Email and Social-Media Impersonation

Fraudulent email and social media accounts are used to deceive users and organisations. Attackers impersonate family, coworkers, or bosses to steal personal information or money. Deepfake technology makes impersonation easier than ever. Criminals can now make realistic photographs, videos, and voicemails.[5] A phoney video of the CEO authorising a transfer to an offshore account deceived the finance staff of a small American company, costing $250,000 in 2021. Impersonation causes financial loss, reputational damage, emotional agony, and legal issues. Businesses risk losing customers' trust if counterfeit SMS are sent with their identity. Reporting fake profiles or emails, validating sender addresses, and enabling multi-factor authentication are crucial. AI-powered monitoring can detect suspicious conversations for businesses.

3.6 Overlapping and Emerging Variants

The bulk of cyber forgery incidents use multiple methods. Phishing can supply altered documents for recruiting fraud and phoney financial instructions. Combining real and bogus data with blockchain, AI, and the dark web creates "synthetic identities" effortlessly. Underground marketplaces provide forged passports and credit cards for undetected foreign activities. Cyber forgeries have evolved beyond signature and document fabrication to multi-layer attacks leveraging automation, social engineering, and AI-powered deepfakes. Continuous research, legislative change, and technological innovation are needed to avoid such threats. Institutions use secure authentication, public awareness campaigns, blockchain credentialing, and AI fraud detection to counter cyber forgeries. Staying watchful, changing passwords often, and double-checking digital messages before acting are advised.

[5] D. Anny. Securing Next-Generation Systems: Deep Learning-Based Approaches to Digital Forgery and Data Breach Detection. 2.025.

4. Causes and Techniques Used

Cyber forgeries thrives on technological weaknesses, human error, and criminal exploitation. We must understand criminal motivations and tools to develop effective preventative and legal actions. The main factors are listed below.

4.1 Use of Malware, Spoofing, and Key loggers

Cyber forgers use malware to steal sensitive data. Malware includes viruses, worms, trojans, spyware, and ransomware.[6] They can steal digital signatures, bank data, login credentials, and personal identification numbers by stealthily infiltrating systems. Once gathered, this information can be used to impersonate the victim, commit financial fraud, or manipulate digital documents. A key logger is malware or hardware that records and monitors keystrokes. Hackers can steal passwords, PINs, and verification codes by capturing every character typed with key loggers. This lets them bypass authentication and falsify documents. Spoofing—impersonating someone else—is another frequent cyber forging strategy.[7] While DNS and IP spoofing drive users to fake portals, email spoofing makes communications look like they came from a legitimate sender. Fraudsters can impersonate reputable companies using caller ID spoofing. Malware, key loggers, and spoofing are often used with social engineering like phishing emails and pop-ups to trick users into downloading hazardous files or disclosing personal information. Integrating methods makes cyber forgeries more successful. User awareness and good cybersecurity regulations become increasingly crucial as detection grows harder.

4.2 Weak Passwords and Human Negligence

Careless or malicious human behaviours can expose even the most powerful security safeguards, enabling cyber forging. Common issues include weak, repetitive, or easy-to-guess passwords. Attackers utilise passwords because users seldom change them or reuse them across platforms. Cybercriminals use brute-force attacks, credential stuffing, and phishing to infiltrate accounts and counterfeit documents. Carelessness extends beyond passwords. Cybercriminals

[6] P Putro, M. Luthfi. An authentic and secure printed document from forgery attack by combining perceptual hash and optical character recognition. In: 2.019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). IEEE; 2.019. p. 1.57-6.2

[7] J. Bakas, R. Naskar, R. Dixit. Detection and localization of inter-frame video forgeries based on inconsistency in correlation distribution between Haralick coded frames. Multimed Tools Appl. 2.019;7.8(4):4.905-3.5.

can gain network access by leaving devices accessible, transferring sensitive documents through insecure channels, or failing to log off of public terminals.[8] Employees may unknowingly send confidential emails or attachments to scammers posing as coworkers or partners. If warning signs like odd URLs or unexpected demands for sensitive information are ignored, forgery attacks are more likely to succeed. Organisational flaws compound the problem. When companies don't update software, handle patches, or establish data standards, they risk systemic hazards. Without proper training, staff may miss phishing, malware, and other data corruption methods. Cybercriminals can forge financial instructions, copy digital signatures, and send phoney messages due to these weaknesses. Automated log-off systems, strong password policies, multi-factor authentication, and education can address human negligence and weak passwords. Cyber forgeries can have major financial, legal, and reputational ramifications; thus, a vigilant workforce and effective organisational procedures are essential.

4.3 Exploiting Software Loopholes

Cybercriminals employ software, OS, and online app weaknesses to falsify documents. Attackers can compromise authentication methods, change records, or insert malicious code into valid files using software vulnerabilities, misconfigured servers, or unpatched faults. Hackers have plenty of time to exploit these weaknesses before anyone notices until a security breach occurs. Security weaknesses in document management or enterprise resource planning systems allow unauthorised parties to change financial data, contracts, or certificates.[9] Online forms that don't check user input can be used by attackers to submit fake photographs, modify metadata, or include malicious scripts. Some cyber forgers utilise obsolete encryption technologies or poorly implemented digital-signature procedures to modify digitally signed documents without alerting anyone or invalidate signatures. Software is reverse engineered by attackers to discover its inner workings and obtain keys or cryptographic secrets.[10] Their expertise in replicating or circumventing security systems allows them to create convincing false credentials, certificates, and authorisation documents. Web applications, financial

[8] DM MY, M. Agustantia, S. Zulaiha. Tindak Pidana Kejahatan Pemalsuan data (Data Forgery) dalam Bentuk Kejahatan Siber (Cyber Crime). J Pendidik Konseling (JPDK). 2.022;4(6):6.635-4.0.
[9] R. Zahoor, N. Razi. Cyber-crimes and cyber laws of Pakistan: An overview. Prog J. Res Arts Humanit. 2.020;2(2):1.33-4.3.
[10] NN Hurrah,NA Loan ,SA Parah, JA Sheikh , Muhammad K, de Macedo ARL, et al. INDFORG: industrial forgery detection using automatic rotation angle detection and correction. IEEE Trans Ind Inform. 2020;17(5):3630-9.

gateways, and e-governance portals are often targeted due to their sensitive data. Preventing software loophole exploitation requires secure coding, security upgrades, patch management, and penetration testing. Intrusion-detection systems, vulnerability assessments, and regular audits help businesses identify and mitigate threats. By correcting these technical issues, institutions can protect sensitive data from modification and reduce cyber forgery risk.

4.4 Role of Organised Crime and Underground Markets

Underground marketplaces and organised cybercriminals have improved cyber forgeries. These networks sell virus kits, phishing templates, forged document bundles, and stolen passwords manufactured by hackers, programmers, and fraud specialists. These marketplaces make sophisticated attack strategies easier for less skilled criminals to commit cyber forgeries by packaging them into user-friendly products. On dark web sites and encrypted forums, many people trade stolen data, software exploits, and forging services. These places accept bitcoin transactions, which protect anonymity.[11] Cross-border networks complicate law enforcement and legal jurisdiction. Individuals, schools, and small businesses may be targeted by international forgeries.

These resources have also accelerated cyber forging procedures. The broad availability of low-cost technologies like deepfake impersonation services and phishing kits allows offenders to commit attacks previously reserved for highly trained hackers. Organised criminal gangs may organise major identity theft, bank fraud, and document forgery operations to maximise earnings or target businesses, governments, or wealthy individuals. Underground markets demonstrate that cyber forging is a systemic crime. To combat this menace, international cooperation, cyber intelligence sharing, and more online platform regulation are needed. Businesses and individuals should establish cybersecurity precautions, authentication processes, and staff awareness initiatives to limit the risks of these criminal networks.

4.5 Emerging Technologies as Double-Edged Swords

Blockchain, machine learning, and AI have transformed digital security by preventing cyber forgeries. These technologies can be used by cybercriminals, making them a benefit and a curse

[11] AA Khan, AA Shaikh, AA Laghari, MA Dootio, MM Rind, SA Awan. Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. Int J Electron Secur Digit Forensics. 2022;14(2):124-50.

for forgeries.[12] The use of AI-driven picture and video synthesis can create deepfakes, which can pass for real individuals in subtle ways. Deepfakes can legitimise transactions, change contracts, or deceive employees and customers, endangering individuals and companies. With machine learning algorithms, phoney identities, signatures, and documents can be created automatically. When attackers mix real and fraudulent personal data to create identities that look real to verification systems, banks, government agencies, and employers struggle to detect fraud. Automated programs that resemble signatures allow forgeries to bypass typical verification procedures. Forgeries can result from misusing legal technology like cloud-based collaborative platforms. Shared digital workspaces, file-editing tools, and document management systems can be used to change contracts, certifications, and documents while appearing legal. Cyber forgeries can occur on platforms without effective authentication, access limitations, and audit logs. A multifaceted approach is needed to reduce these risks. Businesses should utilise AI-powered monitoring systems to detect suspicious activity, use two-factor authentication, and double-check blockchain or cryptography deployments to secure data. Users must be informed about evolving technologies, and developers and politicians must consider ethical safeguards and legislative frameworks to prevent their exploitation. Understanding these technologies' exploitative and protective potential helps stakeholders maximise innovation and reduce cyber crime.

5. Legal Provisions and Case Studies

To combat cyber forgeries, legislators, courts, and international organisations have developed legal tools for investigation, punishment, and prevention.[13] After reviewing major legislative provisions and international activities, this part presents case examples to demonstrate legislation's actual application.

5.1 The Information Technology Act, 2000 (India)

The **Information Technology Act, 2000 (IT Act)** is India's primary legislation dealing with electronic records, cybercrime, and data protection. Several of its provisions directly address

[12] A. Thakur, N. Jindal. Machine learning based saliency algorithm for image forgery classification and localization. In: 2.018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE; 2.018. p. 4.51-6.
[13] SJ Djamshedovich. Analysis of objective and subjective elements of the crime of document forgery, selling, or using forged documents. Am J Polit Sci Law Criminol. 2025;7(04):23-8.

offences linked to cyber forgery:

- **Section 65** penalises tampering with computer source documents, ensuring that original program codes or data cannot be altered unlawfully.

- **Section 66C** prescribes punishment for identity theft, including fraudulent use of electronic signatures, passwords, or other unique identification features.

- **Section 66D** deals with cheating by personation through communication devices or computer resources, which covers impersonation in forged e-mails, social-media accounts, and phishing scams.

- **Section 67A** and **Section 72** impose penalties for publishing or disclosing information without consent, which may accompany acts of forgery (Gowda & Pawar, 2023).The Act recognises electronic signatures as valid, provided they comply with prescribed security standards such as public-key infrastructure (PKI) and secure hash algorithms.[14] Amendments in 2008 strengthened penalties and introduced provisions on data privacy, intermediary liability, and cyber terrorism, broadening protection against forgery-related offences.

5.2 The Role of Conventional Laws in Cyber Forgery

While earlier cases referenced the Indian Penal Code (IPC) provisions for forgery, the IT Act now largely supersedes these for cyber-related offences. In practice, courts predominantly rely on IT Act provisions for investigating, prosecuting, and adjudicating cases involving electronic forgery, identity theft, phishing, and manipulation of digital documents. Conventional IPC provisions may still apply in limited scenarios, such as offline forgery or offences intersecting with traditional criminal law, but are no longer the primary legal tool for cyber forgeries.

5.3 International Frameworks: The Budapest Convention

The historic Budapest Convention, also known as the Council of Europe Convention on Cybercrime, aimed to harmonise national laws and foster international cooperation against cybercrime and forgery States that sign it must criminalise computer forgeries, unauthorised

[14] P. Rachana, BS Bharath. Copy-Move Forgery Localization Using DCT With LoG Filter. In: 2.023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE; 2.023. p. 6.58-6.4.

access, data interference, and system interference. The treaty promotes cross-border evidence sharing and faster data retention to track and prosecute offenders.[15] India hasn't signed the treaty, but its laws and cybersecurity strategy are influenced by it. UNODC guidelines and other tools can assist governments build successful laws.

5.4 Real-Life Examples and Judgments

a) Phishing Scam Targeting a Bank (India)

A group used phishing emails to obtain login credentials from hundreds of Indian bank users, attracting attention. After constructing bogus banking websites to steal credentials, the crooks transferred money to mule accounts. In addition to the BNS' forgery and cheating laws, law enforcement cited IT Act Sections 66C and 66D. Cyber cells' quick response, which partially recovered stolen monies, showed the necessity of coordinated inquiry.

b) Fake Academic Certificates Case

A multistate ring sold bogus degrees to online job seekers. The accused was charged with utilising falsified documents under BNS Sections 335-340 and defrauding through computer resources under IT Act Section 66D. Courts have stressed the need of companies using secure gateways to validate digital certificates.

c) International Case: Deepfake Video Forgery

A European criminal gang pretended to be the company's CEO in a video conversation and ordered an employee to send a lot of money to an offshore account. The Budapest Convention was used to request international collaboration in the arrests.[16] The case emphasised the growing threat of AI-enabled forgeries.

d) Delhi High Court on Electronic Records (India)

The Delhi High Court considered admitting emails and call logs despite the main accusations

[15] S. Ranjan, P. Garhwal, A. Bhan, M. Arora, A. Mehra. Framework for image forgery detection and classification using machine learning. In: 2.018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE; 2.018. p. 1-9.
[16] YE Riany , F. Utami. Cyberbullying perpetration among adolescents in Indonesia: the role of fathering and peer attachment. J. Int Bullying Prev. 2.025;7(1):1.3-2.7.

being terrorism.[17] The decision confirmed that Section 63(4) of the Bhartiya Sashaya Adhiniyam, 2023 requires certified copies of electronically altered or manufactured evidence for admissibility. Cyber forgery prosecutions now centre on this.

6. Preventive Measures & Best Practice

Digital security requires preventative measures as cyber forgeries become more sophisticated. Technology improvements, user education, and corporate control are needed to reduce risks and protect sensitive data. This section outlines critical steps people, organisations, and organisations can take to prevent forgeries.

6.1 Strong Authentication: Two-Factor and Biometric Systems

Users need strong authentication to prevent cyber forgeries. Thus, only authorised individuals can access sensitive data and systems. Two-factor authentication (2FA) increases security beyond a password by requiring two verification methods. An authentication method often includes a password or PIN and a one-time code (SIM, email, or app generated). Even if a hacker gets a password through phishing, malware, or key logging, two-factor authentication (2FA) prohibits unauthorised access because the hacker cannot access the second factor. In addition to two-factor authentication, biometric authentication uses physiological traits like fingerprints, facial patterns, and iris structures to provide additional security.[18] Biometric systems are great for banking, commercial networks, government portals, and e-governance applications due to their security and inability of replication or fabrication. Modern biometric technology like multi-modal authentication, which combines fingerprint and facial recognition, protects against identity fraud and fraudulent transactions. If authentication techniques are strong, users will trust digital platforms and their personal data.[19] Businesses should ensure authentication methods work with their software, update them frequently, and train personnel on their use. Multiple levels of protection, including 2FA or biometric authentication, encryption, access limits, and anomaly detection, dramatically diminish criminals' ability to commit fraud. Effective authentication is crucial to protecting personal and corporate assets

[17] S. Pajankar. Cyber crimes and cyber laws in India. Delta J. Natl Multidiscip Res. 2.020;7(1):2.5-9.
[18] A. Gaurav, BB Gupta, S. Bansal, KT Chui. Forgery Detection Based on Deep Learning for Smart Systems: Recent Advances and Collection of Datasets. Digit Forensics Cyber Crime Investig. 2.024:1.96-2.10.
[19] P. Rachana, BS Bharath. Copy-Move Forgery Localization Using DCT With LoG Filter. In: 2.023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE; 2.023. p. 6.58-6.4.

from fraud and other cyber threats in the digital era.

6.2 Digital Signatures and Encryption

Digital signatures, a crucial cybersecurity component, are one of the best ways to fight cyber frauds. They produce a unique code mathematically linked to the document's signer via cryptography. This ensures the document's authenticity (from the stated sender) and integrity (not altered in transit). Since the digital signature becomes invalid when the document is changed, forgery is easily recognised. Digital signatures are legally enforceable in several countries, notably India's Information Technology Act, 2000 and the US' ESIGN Act, making them crucial to cybercrime prevention.[20] Encryption and digital signatures protect sensitive data. The right decryption key is needed to read encrypted data, which is encoded using complex methods. Common applications include SSL/TLS online communication security, end-to-end encryption in messaging systems, and AES file storage. These measures prevent hackers from intercepting, duplicating, or modifying data in emails, documents, and digital transactions. To maintain security, organisations should rotate keys frequently, store them securely, and update cryptographic methods quickly. Regular audits and system updates are needed because attackers can use weak encryption to bypass protections. Users must also learn to handle cryptographic keys, identify encrypted channels, and verify digital signatures. Digital signatures and encryption in corporate and personal workflows reduce document manipulation, identity fraud, and unauthorised access. An integrated cybersecurity strategy with authentication and organisational norms comprises several tools to prevent cyber forging.

6.3 User Awareness and Training

Human error can defeat cyber forgeries even with cutting-edge technology. Regular user awareness campaigns and training sessions are needed to teach the public, students, and employees about cybercriminals' social engineering, spoofing, and phishing methods. When trained to spot suspicious messages, verify the sender, and avoid risking important data, people can better protect it. Training programs should emphasise phishing detection, URL verification, avoiding public Wi-Fi networks, and login credential protection.[21] Two-factor authentication,

[20] R. Gowda, D. Pawar. Deep learning-based forgery identification and localization in videos. Signal Image Video Process. 2.023;1.7(5):2.185-9.2.
[21] T. Miao, Zifang MA, Zhongyu XUE, S. Yaqiong, Zhenya LI, W. Qingwen, et al. Correlation between experience of childhood abuse and implementing cyberbullying in college students. J. Chin Sch Health. 2.020;4.1(1):8.2-5.

strong passwords for each account, and caution while downloading and opening attachments should also be stressed to participants. Report irregularities or suspected assaults immediately to help firms respond quickly and prevent modest security breaches from becoming major incidents. Awareness programs include interactive quizzes, posters, newsletters, simulation exercises (such mock phishing attempts), online courses, workshops, and simulations. These methods keep one alert and reinforce learning. Because employees are the first line of defence against fraud, companies that promote cybersecurity knowledge reduce forgeries.[22] Training must be updated often due to emerging threats including synthetic identities, AI-created deepfakes, and dark web marketplace phishing kits. Employee education and technology precautions like encryption, multi-factor authentication, and monitoring help reduce cyber fraud. In addition to technological protections, educated and vigilant users are the best defence against hostile exploitation of personal, business, and government digital assets.

6.4 Organisational Policies and Governance

Comprehensive organisational policies are the best barrier against cyber forgeries and the best means to ensure business-wide compliance. Policies should cover document verification, electronic signatures, digital data storage, and audits. Codifying these protocols gives organisations structure, which reduces uncertainty and boosts security. Governance uses access control. Least-privilege models and role-based access rights might restrict stakeholders and employees to the information they need. This prevents internal or accidental forgeries and protects crucial data. Organisations should also have secure backup systems to restore data after tampering and incident response protocols to detect, report, and mitigate forgeries. In real time, anomaly detection systems and other continuous monitoring solutions alert administrators to unusual conduct, allowing them to act. Frequent audits and risk assessments reveal security vulnerabilities before hackers do.[23] These assessments should include software security, encryption protocol verification, and authentication method testing. Collaboration with cybersecurity experts, law enforcement, and regulatory agencies improves organisational readiness and aligns best practices with shifting threats and legal requirements. Encourage employee responsibility and cybersecurity awareness to support policy adherence. Cyber forgery defence requires strong governance and established organisational rules in the digital

[22] MS Hossain, G. Muhammad, Al M. Qurishi. Verifying the images authenticity in cognitive internet of things (CIoT)-oriented cyber physical system. Mob Netw Appl. 2.018;2.3(2):2.39-5.0.
[23] CI Mallik, RB Radwan. Adolescent victims of cyberbullying in Bangladesh-prevalence and relationship with psychiatric disorders. Asian J Psychiatry. 2020;48:101893.

world. When regularly enforced and clearly explained, these policies preserve sensitive information and boost the institution's credibility. They protect data and trust via technical safeguards, user training, and laws.

6.5 Emerging Technologies in Prevention

Blockchain and AI secure digital assets and transactions, preventing cyber forgery. AI-driven systems can detect forgeries in user actions, document changes, and transactions. In real time, machine learning algorithms can identify suspicious activity such inconsistent document change trends, unexpected login locations, and unusual access times. Such situations allow prompt intervention. AI-assisted fraud detection can check transaction data for unusual activity in financial systems.[24] Blockchain's immutability adds security. Every blockchain update is recorded and verifiable across all nodes, so businesses can be sure any unlawful alterations to digital assets, certifications, or contracts will be exposed. Verifying academic qualifications, processing legal documents, and validating supply chains require openness and confidence, hence, this quality is useful. Cloud-based digital identity systems are popular for protecting massive authentication and verification operations. These technologies help organisations validate user credentials and decrease forgery using safe enrolment, multi-factor authentication, and tamper-evident identity data storage. Universities, corporations, and governments benefit from digital certificate verification and remote approval. Integration of these technologies into organisational processes produces a multilayered protection. Strong authentication, encryption, user education, governance, and new technology can avoid cyber forgeries. Cloud-based solutions, artificial intelligence (AI), and blockchain technology can proactively identify, prevent, and respond to forgery attempts to protect sensitive data like financial, legal, and personal information and ensure trust and operational integrity in the digital age.

7. Suggestions / Recommendations

Cyber forgery prevention and combat require more than technical security. Policy actions, public involvement, and stakeholder coordination are as crucial as strong authentication, encryption, and organisational policies. We propose the following improvements to prevention

[24] R. Ashraf, MS Mehmood, T. Mahmood, J. Rashid, Nisar MW, M. Shah. An efficient forensic approach for copy-move forgery detection via discrete wavelet transform. In: 2.020 International Conference on Cyber Warfare and Security (ICCWS). IEEE; 2.020. p. 1-6.

and rectification frameworks to meet the growing threat of cyber forging.

7.1 Need for Stricter Laws and Speedy Trials

Strong laws prevent cyber forgeries. India's Information Technology Act, 2000 and pertinent elements of the Bhartiya Nyay Sanhita (BNS) establish prosecution, but digital technology and advanced forging tactics necessitate modifications and harsher sanctions. Current legislation fail to address new threats like deepfakes, artificial intelligence-generated identities, and blockchain-related forgeries, allowing offenders to take advantage of gaps. Effective deterrence requires law reform and fast trials. Cybercriminals gain confidence when prolonged litigation reduces penalties. Cybercrime cells or cyber courts can streamline adjudication. The courts can quickly handle cases involving digital evidence, e-signatures, and bitcoin transactions to ensure that offenders are punished and victims receive justice.[25] Judges, prosecutors, and law enforcement officials must be trained in digital forensics and cybercrime investigation to properly apply laws and analyse electronic evidence.

7.2 Public Awareness Programs

Human mistake enables cyber forgeries. Naivety about secure passwords, personal information exchange, and phishing/spoofing can be used by criminals. Thus, prevention relies significantly on public awareness. Seminars, online courses, webinars, and mass-media campaigns teach internet safety.[26] These can teach children to spot bogus communications, verify websites, use strong passwords, and handle digital files carefully.[27] Cybersecurity awareness should be taught in schools, businesses, and communities to foster a culture of alertness. Awareness efforts should also address new threats like deepfakes, AI-created identities, and complicated social engineering to enable the public spot and report potential incidents.[28] Education is the first line of protection against cyber forgeries; it reduces attack success and promotes safe online behaviour.

---

[25] J. Zhang, H. Hu, S. Huo. A browser-based cross site request forgery detection model. J Phys Conf Ser. 2.021;1.738(1):012.073.

[26] R. Pandey, AKS Kushwaha. A Novel Histogram-Based Approach for Video Forgery Detection. In: 2.024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI). IEEE; 2.024. p. 8.27-3.0.

[27] A. Gaurav, BB Gupta, S. Bansal. Forgery Detection Based on Deep Learning for Smart Systems. Digit Forensics Cyber Crime Investig Recent Adv Future Dir. 2.024:1.96.

28 P. Kour. A Review on Cross-Site Request Forgery and its Defense Mechanism. 2.020

7.3 Collaboration Between Tech Companies and Law Enforcement

One agency cannot prevent or prosecute cyber forgery. IT businesses and police departments must collaborate to detect, report, and mitigate threats quickly. Payment processors, social media [29]sites,[30] and ISPs should report suspicious activity, malware outbreaks, and phoney accounts to authorities. Cyber forgery responses can be coordinated through collaborative task forces, threat intelligence-sharing platforms, and public-private collaborations. Collaboration allows stakeholders to standardise verification techniques, discover software vulnerabilities, and enforce accountability. Multinational coordination is essential to counteract cross-border forgeries. Effective prosecution of cybercriminals requires international collaboration, extradition treaties, and a solid legal framework due to poor enforcement in many jurisdictions. An integrated network between commercial IT corporations and law enforcement agencies enables proactive prevention and faster response.

7.4 Integration of AI-Based Fraud Detection Tools

Machine learning (ML) and artificial intelligence (AI) improve cyber forgery detection and prevention. AI systems can track user behaviour, transactional trends, and submissions to detect document forgeries. AI algorithms can detect digital signature abnormalities, strange login times, and questionable transaction amounts. They can also detect manipulation in deepfake movies, images, and audio and warn of fraud in real time. AI-driven monitoring systems can help banks, e-governance, and businesses prevent fraud. Effective counterfeit detection requires frequent system updates to combat more complicated approaches. Combining AI with encryption, multi-factor authentication, and organisational laws creates a multi-layered security solution. Combining AI-based detection with continuous staff training improves response time to emerging threats, reducing financial, reputational, and legal concerns.

7.5 Additional Recommendations

Beyond the above measures, a few complementary strategies can further strengthen cyber forgery prevention:

[29] PM Raju, MS Nair. Copy-move forgery detection using binary discriminant features. J King Saud Univ Comput Inf Sci. 2022;34(2):165-78.
[30] R. Gowda, D. Pawar. Deep learning-based forgery identification and localization in videos. Signal Image Video Process. 2.023;1.7(5):2.185-9.2.

1. **International Cooperation:** Encourage cross-border data sharing and unified legal frameworks to tackle cyber forgery operating globally.

2. **Research and Development:** Invest in developing advanced forgery detection tools, including AI-driven document verification and biometric authentication improvements.

3. **Incident Reporting Mechanisms:** Establish user-friendly platforms for reporting suspicious activities, helping authorities act quickly on potential forgery attempts.

4. **Periodic Policy Review:** Organisations should periodically review and update internal policies, access controls, and authentication protocols to remain resilient against evolving threats.

8. Conclusion

Today's digital world includes identity theft, phishing, online signature forgery, credit card and banking fraud, document and certificate manipulation, email or social media impersonation, and cyber forging. Cyber forgery investigation found that technology has improved efficiency and convenience, but also created security weaknesses that cybercriminals can exploit. Human error, poor password practices, software vulnerabilities, malware, keyloggers, and spoofing are major causes. National and international laws must handle these challenges. The Information Technology Act, 2000, the Indian Penal Code, and the Budapest Convention enable prosecution, deterrence, and international cooperation. Real-world case studies show how cyber forgeries can penetrate complex systems owing to inadequate security or human error. Protecting sensitive data and digital transactions requires proactive measures. Biometric and two-factor authentication, digital signatures, encryption, and AI-based monitoring are needed. User training, strong organisational policies and governance, and continual threat monitoring help avoid forgeries. Mitigation options include stricter laws, faster courts, public awareness campaigns, tech company-law enforcement alliances, and AI-based fraud detection systems. Finally, to resist cyber forgeries, one must grasp their forms, sources, and effects. This involves social, legal, and tech collaboration. We must be cautious, educate ourselves, adopt secure digital habits, and enforce laws to make digital places safer, less appealing for thieves, and more trustworthy. Security, regulatory, and public awareness strategies must be regularly updated to reduce cyber forgery risks and maximise digitisation benefits without being eclipsed by fraud.