Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 03 ISSUE 4, 2025

Reducing Electronic Blackmail and its Relationship to Modern Technologies

Maryam Hsaini
Babylon Education Directorate / Al – Baqer high school for girls
mariam.almosewy@gmail.com

Abstract:

Electronic blackmail crime refers to one of the most dangerous crimes which result in victim many harms, if in reputation/personal life in his work. Cyber extortion and electronic blackmail became an increasing issue in digital era, aiming at firms and persons via threats of operational disruptions, reputational damage, data breaches. Present paper explores relation among new technologies and growing electronic blackmail prevalence. Through reviewing present paper, recognizing the main technologies which facilitate these crimes, analyzing efficient mitigation strategies, present paper targets at presenting general perspectives into combating electronic blackmail in evolving technological area.

Keywords: Electronic blackmail, cyber extortion, digital security, modern technologies, data breaches, cybersecurity threats, mitigation strategies.

1. Introduction

Information technology deployment resulted in profound society shifts. Developed access to internet ruined presented sequence in whole regions, containing cultural, economic, legal, social regions. Internet access had obvious positive effects on society, however negative, one of which refers to raise in cybercrime rate. Budi Raharjo describes cybercrime as the function which violates the rule using technology of computer which uses internet technology [1]. Cyber-attacks rate developed as the world relies on communication and interaction with others via digital platforms. Cybercriminals apply a lot of tactics for stealing data of social media user, like blackmail, fraud, ransomware, malware, so on. Dividing private data with other users on social media develops showing sensitive and personal content risk associated with people that causes in info leakage. Currently, online blackmail has considerably developed, such increment was monitored by a lot of authorities in the UK and Europe [2].

In digital world of nowadays, decreasing cyber extortion significance is felt more than ever before because of developing persons and firms' reliance on developed technologies. Cloud systems, social networks and internet development resulted in big personal and organizational info amount for being saved and transferred online. Such reliance on digital era presented novel chances for cybercriminals to aim at their victims by threatening for disclosing inflict psychological and social harm, sensitive info, extort money. In another word, new technologies development like IOT, AI, encryption could strengthen cybersecurity, when abused, become a mean for complicating attacks. Cyber extortion is not just a threat to info security, however could have broaden economic effects on businesses and devastating psychological impacts on persons. So, recognizing present issues and presenting efficient solutions for decreasing the threat is taken one of the significant priorities in cybersecurity domain [3].

Electronic blackmail, called cyber extortion, includes threatening firms/persons for damaging reputations, reducing sensitive data, disrupting tasks, till particular needs are faced. Such crime type surged with quick digital technologies development. Raising dependence on social media platforms, internet, mobile devices made novel vulnerabilities, making it simpler for cybercriminals to exploit victims.

Undoubtedly, Electronic Blackmail is taken as one of the most dangerous Cybercrimes committed in contrary to people, easily due to that Blackmail considerably impact an individual's security sense, arousing fear and dismay inside Victim. In another word, sometimes, Perpetrator commits his Crime with high audacity, believing that recognizing the identity will be hard, in case that is possible. In addition, he is really convinced that his secrets are enough for guaranteeing that Victim would surrender to his needs. Also, Blackmail, in several samples, may force Victim to commit suicide because of being under permanent threats pressure and endless needs from Perpetrator/often that can be the result of exposing his secrets on Social Media, where info/news will be slowly broaden between people causing the unstoppable scandal [4].

Present paper goal is presenting general cyber-extortion overview and its relation with new technologies. This paper tries to explore different solutions which could be taken for mitigating and combating this threat kind via novel technologies' usage like AI, blockchain, cryptography. That analyzes legal and social concerns related to cyber-extortion and evaluates such technologies' role to promote cybersecurity and avoiding these crimes.

2. Background

For comprehending electronic blackmail dynamics, this is important to explore the evolution. Traditional extortion has considerably transformed with novel technologies' advent. Cybercriminals use essential methods like phishing models, social engineering tactics, ransomware attacks. Dark web and cryptocurrency proliferation has made unusual transactions facilitated and complicate rule enforcement attempts.

Cyber extortion contains different threats' kinds where criminals utilize Internet/digital technologies for extorting victims through threatening to disclose private info/ ruin individual/organizational systems. A usual extortion kind is sextortion, where criminals threaten victims with providing their private info/pictures, particularly when they are in personal situations [5]. In such extortion kind, victims are normally pressured to pay money/services in exchange to maintain the personal info private. The other cyber extortion kind refers to ransomware, where hackers have access to a victim's computer systems/private info and lock/encrypt them. After that, victim is asked to pay a ransom to have access to data/systems again [6]. Phishing refers to other usual electronic extortion kind where criminals utilize unoriginal websites/ emails to trick victims in providing sensitive info to them like credit card numbers, passwords/other private data. In such attacks' kinds, criminals sometimes pose as legal entities, like banks/service organizations, also ask victims to enter their info in unoriginal sites. Such various electronic extortion kinds pose a lot of threats to private and

organizational security and need preventive scales and general awareness for avoiding the damage [7].

As time has passed and cyberattacks became important, more considerable techniques entered electronic extortion. Now, presenting technologies like AI as well as ML are applied for diagnosing and analyzing behavioral attacks' models, therefore criminals apply such means for modelling more targeted and considerable attacks. Blockchain entered as novel technology in electronic extortion prevention, since the attributes of security could be helpful to record and confirm transactions and sensitive info.

Generally, electronic extortion evolved from simple threats to complicated and aimed attacks which apply developed technologies. Historical trends illustrate that for countering such threats, this is essential to have developed security strategies, educate and increase users' awareness, enhance novel technologies for diagnosing and avoiding attacks.

New technologies have an important role to facilitate/ counter cyber-extortion threats. On the one hand, such technologies could provide hackers and cybercriminals developed abilities for modelling more considerable attacks, however in another word, novel means and techniques exist for recognizing, avoiding, and countering such threats which aid strengthening digital security. There are several new technologies which are efficient here:

Blockchain: Blockchain technology, applying decentralized and transparent structure, could be helpful to avoid cyber-extortion and info extortion. In blockchain-based systems, transactions are safely recorded and no unauthorized shifts/ manipulations could be used to data. Such attribute applies blockchain efficiently to guarantee security in online payments and transactions, particularly in contrary to digital extortion. Also, blockchain could be used to save sensitive info in encrypted and safe manner, with no requirement to trust central institutions [8].

Artificial Intelligence and Machine Learning (AI & ML): AI and ML could aid recognizing behavioral models in cyberattacks and electronic extortion. Through analyzing data and identifying suspicious manner, such technologies could diagnose sextortion, ransomware, phishing attacks before they occur. ML patterns could be continuously trained and updated with novel data to simulate and diagnose emerging attacks. For instance, unusual diagnosis mechanisms could recognize uncommon models in network traffic/online task which might show an attack [9].

Cryptography: Encrypting info refers to one of the most efficient paths for avoiding electronic extortion threats. Robust encryption technologies could secure sensitive and personal info from unauthorized access and disclosure. In ransomware attacks, hackers normally encrypt files for forcing victims to pay a ransom. Applying developed encryption, firms, persons could save their info in a way that makes that unusable when criminals would have access to data [10].

Two-Factor Authentication (2FA): Two-factor authentication refers to technique of security which is considerably efficient to decrease electronic extortion threat. Such technology lets users to apply second agent (like the code sent to mobile phone/email) for accessing their accounts, in addition to their password. The technique guarantees that even if a user's login info is illegally achieved, the attacker would not have access to account [11].

Big Data Security Analytics: Big Data Analytics lets means of security for analyzing big data amounts in real time. Such analytics could aid identifying potential threats to networks and systems. Huge Data technologies could aid recognizing more important attacks like targeted ransomware and developed phishing which might be hard for comfortably diagnosing [12].

Cloud Security Technologies: Applying cloud services as the safe option for data storage and resource management became one of the most broadly applied techniques. Persons and firms could take advantage of cloud services to save the info applying developed security systems like threat

diagnosis, encryption, traffic controlling. In presence of attack on data in cloud services, security technologies could rapidly recover data and avoid info loss [13].

Generally, new methods have an important role to combat cyber extortion, however individuals and firms yet require to efficiently apply such technologies and continuously update them for countering more important and new attacks.

3. Modern Technologies' Role

New technologies have dual role in electronic blackmail:

- **Social Media Platforms:** Cybercriminals exploit social media for collecting personal info, spread bad content, recognize potential victims. Sextortion, blackmail, extortion are sometimes interchangeably applied with various meanings. Extortion includes violence use/threat for achieving money/valuables, when blackmail depends on coercion through threatening to expose sensitive info on victim. Online extortion normally includes threats for damaging assets/ data, while online blackmail threatens to present info which can damage victim's reputation. Sextortion refers to particular blackmail kind which applies sexually obvious content to manipulate victims. Blackmail on social media is becoming increasingly usual. Sensitive info is sometimes achieved via hacking, user negligence/deceiving users in showing private details. Research show that 6–8% of Czech youth (aged 8–17) experienced blackmail on social media. In Saudi Arabia and Oman, blackmail cases considerably increases, with perpetrators needing money, sexual favors/other services. Reports from Gulf Cooperation Council (GCC) bold that 80% of blackmail victims in area are women, with over 30,000 cases reported per year. Child victims are especially vulnerable, as predators apply obvious material to need later money, content/sexual exploitation. Blackmail results could be strict, influencing the two mental health and social reputation. Victims might suffer from social isolation, depression, anxiety, suicide in severe cases. Children might experience nervousness, self-blame, academic struggles, low self-esteem, nightmares. In spite of such risks, a lot of people remain vulnerable to blackmail because of their tendency to share sensitive info online [14].
- **Mobile Devices:** smartphones and apps ubiquity enhance exposure to phishing attacks and malware infections. Mobile devices have important role in electronic blackmail increment, presenting both chances for perpetrators and vulnerabilities for victims. With broad smartphones and tablets usage, users save and share big personal info amounts, making them potential targets for cybercriminals. The main way mobile devices contribute to electronic blackmail is via access to sensitive data, such as financial details, photos, videos, messages. A lot of individuals sync their mobile devices with cloud storage/social media accounts, raising data breaches' risk. Hackers could exploit poor passwords, phishing attacks/malware to obtain unauthorized access to a victim's personal content. While achieved, such data could be applied for blackmail, with perpetrators threatening to present compromising info unless needs are met. Also, mobile devices make real-time communication facilitated that cybercriminals apply for quickly pressuring victims. Emails, messaging apps, social media direct messages serve as usual platforms for blackmailers to deliver threats. Internet anonymity lets criminals to act with little fear of being recognized, making electronic blackmail more prevalent. Sextortion, an electronic blackmail kind including obvious content, is specially joined to mobile device use. A lot of victims unknowingly share intimate images via messaging apps/video calls, just to be later threatened with general exposure. It became broadly usual among teenagers and young adults who engage in digital interactions with no completely taking risks into account. In addition, mobile devices are sometimes applied to record and share content, often with no users' knowledge/consent individuals included. It makes chances for blackmailers for exploiting personal moments achieved via hacked devices, social engineering tactics, hidden cameras [15].

- **Cloud Computing:** When proposing convenience, cloud services have security risks when not accurately controlled, causing data breaches. Cloud computing has important role in electronic blackmail, two as a target for cybercriminals and as a mean to save and share sensitive info. As more individuals and organizations depend on cloud services to save financial records, confidential documents, personal data, cyber threats' risk, containing blackmail, has developed. One of the basic ways cloud computing contributes to electronic blackmail is via data breaches. Cybercriminals could exploit security vulnerabilities in cloud storage systems for obtaining unauthorized access to sensitive files, containing private conversations and photos, business documents. When achieved, data could be applied to blackmail users/firms through threatening to expose/eliminate crucial info unless needs are met. The other main issue is ransomware attacks, that hackers encrypt cloud-stored data and need ransom for provision. When victims could not afford, they risk losing permanent access to essential files. Such extortion kind became broad concern, particularly for businesses which depend on cloud-based services for daily tasks. Also, cloud computing makes criminals able to save and anonymously share blackmail material. Blackmailers could upload stolen/sensitive data to encrypted cloud servers, making that hard for authorities to track/eliminate content. It lets them to exert on-going pressure on victims, threatening to provide ruining info unless their needs—if financial/otherwise—are met [16].
- **Cryptocurrencies:** Anonymity presented by digital currencies such as Bitcoin makes it challenging for tracing transactions associated with blackmail payments. Cryptocurrencies have essential role in electronic blackmail through presenting cybercriminals with an untraceable, safe, anonymous technique of receiving payments. The decentralized cryptocurrencies' aspect, like Bitcoin and Monero, makes them attractive for blackmailers who need ransoms in exchange for not presenting sensitive info. One of the basic reasons criminals prefer cryptocurrencies in blackmail models refers to tracing transactions' difficulty. Against traditional banking systems, where transactions are observed and regulated, cryptocurrency transactions happen on blockchain networks, sometimes with no showing sender and receiver IDs. Such anonymity lets blackmailers to act with no fear of prosecution/diagnosis. The other way cryptocurrencies make electronic blackmail facilitated is via ransomware attacks. Here, cybercriminals encrypt victims' data and need payment in cryptocurrency to restore access. As cryptocurrency transactions are not reversible, victims who pay ransom have not any guarantee which they would have access to the files again, making them more vulnerable to later extortion. Also, dark web marketplaces increment made it simpler for criminals to organize and run blackmail models. A lot of cybercriminals buy and sell stolen data, hacking tools, and blackmail services applying cryptocurrencies, making electronic blackmail more broad and essential. To combat cryptocurrency-based blackmail, law enforcement agencies are developing blockchain analysis methods to trace illicit transactions. Although, users and firms should take preventive scales, like applying robust cybersecurity tasks, preventing sharing sensitive data online, and being cautious of phishing efforts which can cause in extortion efforts [17].

4. Strategies for Decreasing Electronic Blackmail

Mitigating electronic blackmail needs multi-faceted strategy:

- **Technical Scales:** Performing strong cybersecurity protocols, like encryption, multi-factor authentication, firewalls. Electronic blackmail refers to increasing cyber threat which exploits digital vulnerabilities to extort victims. Performing robust technical scales that considerably decrease becoming a target risk. One of the most efficient strategies is applying multi-factor authentication (MFA) and robust, unique passwords for avoiding unauthorized access to accounts [18]. Also, data encryption is important to protect sensitive info, both while saved and transmitted, guaranteeing that when data is intercepted, that remains unreadable to attackers. Common backups saved offline could aid mitigating ransomware attacks effect, avoiding

victims from losing crucial files. The other critical scale is installing anti-malware and cybersecurity means for diagnosing and blocking threats like ransomware, phishing, spyware. Firewalls, real-time security alerts, intrusion detection systems (IDS) could aid recognizing and preventing task before it escalates into blackmail [19]. On social media, privacy adjustments must be set for limiting private info visibility, decreasing data risk harvesting by cybercriminals. Also, making location tracking and being cautious of fraudulent messages unable could avoid social engineering attacks which cause in blackmail. Users and firms applying cloud services must adopt zero-trust security models and normally audit access permissions to avoid unauthorized data breaches. Blockchain-based security solutions could develop digital transactions and communications, decreasing vulnerabilities to cyber extortion. In addition, dark web observing means could aid diagnosing leaked private info, letting victims to take proactive scales before it is applied for blackmail. At last, having a cyber incident response plan in place is important to control blackmail efforts effectively. Victims must report threats to law enforcement/cybersecurity agencies than complying with needs. Through integrating robust authentication, privacy protection, encryption, security controlling, users and firms could considerably decrease exposure to electronic blackmail and develop general cybersecurity [20].

- **Awareness and Education:** Educating users and firms on cybersecurity best functions to identify and prevent potential threats. Enhancing awareness and educating users on electronic blackmail is important to avoid cyber extortion. A lot of victims fall prey to blackmail because of knowledge shortage on online security threats and safe digital tasks. Performing awareness campaigns could aid letting people know on risks of sharing sensitive info online and how cybercriminals exploit private data for blackmail [21]. Community organizations, schools, workplaces, must perform training plans of cybersecurity for educating users about recognizing and preventing blackmail efforts [22]. One of the main strategies is enhancing digital literacy, guaranteeing users comprehend how their online tasks could make them vulnerable. People must be trained on significance importance of privacy adjustments, identifying phishing efforts, risks of engaging in risky digital manner, like sharing intimate content online [23]. Particular focus must be located on educating young people, as they are more probably to be targeted for sextortion and social media-based blackmail. The other critical nature is teaching safe online communication habits. Individuals must be encouraged to prevent sharing sensitive info with unfamiliar individuals, be cautious on accepting friend needs from foreigners, refrain from transferring obvious/private content online [24].
- **Legal Frameworks:** Strengthening cybercrime laws and fostering international cooperation to combat cross-border cyber extortion. A strong legal architecture is important in combating electronic blackmail through launching clear rules, penalties, enforcement algorithms. Governments around the world should perform and continuously update cybercrime rules to consider emerging threats in digital extortion. Such rules must describe sextortion, electronic blackmail, extortion as important offenses with severe legitimate results for deterring potential offenders [25]. A main strategy is criminalizing electronic blackmail via particular legislation which contains strict penalties for offenders. A lot of countries have enacted laws which organize cyber extortion as a punishable crime, with penalties ranging from hefty fines to long-term imprisonment. Although, because of global cybercrime aspect, a requirement exists for international cooperation in law enforcement. Cybercriminals sometimes act across borders, making it essential for countries to collaborate via treaties and joint investigations to track and prosecute offenders [26]. The other critical nature is strengthening law enforcement abilities by presenting authorities with developed means and training to examine cyber extortion cases efficiently. Governments must establish cybercrime parts equipped with digital forensics experts who could support victims, track blackmailers, analyze cyber threats. Also, authorities

must closely work with technology companies, internet service providers, and social media platforms for observing and avoiding cyber extortion tasks [27].

- **Incident Response Plans:** Improving general response strategies to control and mitigate blackmail efforts' effect. The efficient incident response plan (IRP) is critical to decrease electronic blackmail effect through presenting structured strategy for controlling and mitigating cyber extortion threats. Having a well-prepared response approach lets firms, users, businesses for fast and efficient reaction, reducing potential damage and avoiding later exploitation. The first stage in incident response plan is early diagnosis and reporting [28]. Individuals and employees must be trained to identify blackmail efforts, such as threats to present sensitive info/needs for ransom. Firms must launch obvious reporting algorithms that victims could confidentially report blackmail incidents to law enforcement, trusted authorities, cybersecurity teams. It guarantees that the concern is promptly considered before it escalates. As blackmail effort is diagnosed, the next stage is containment and evaluation [29]. Security teams/victims must quickly evaluate aspect and threat severity, assigning if attacker already had access to sensitive info/is bluffing. Performing data recovery scales, like retrieving backups/restoring compromised accounts, could aid restricting ruin. Victims must prevent straightly engaging with blackmailer, as impulsively responding might worsen condition. Robust mitigation and response strategy is important to control electronic blackmail efficiently. It contains developing security protocols, like shifting compromised passwords, making multi-factor authentication able, scanning devices for malware/unauthorized access. When financial needs are made, victims must refrain from making payments, as it sometimes encourages extortion. Instead, cybersecurity professionals and legal authorities must be included to investigate and take proper action [30].

5. Challenges and Future Directions

In spite of cybersecurity developments, concerns persist:

- **Rapid Technological Evolution:** Emerging technologies such AI and IOT define novel risks of security. Quick technology evolution provides important issues in combating electronic blackmail. As cybercriminals have access to developed means such as AI, ML, deepfake technology, they could perform important attacks, making it more difficult to diagnose and avoid blackmail. Increasing dependence on IoT devices, cryptocurrencies, cloud computing enhances vulnerabilities' number which could be exploited, proposing blackmailers more entry points to access sensitive info and need ransoms. In addition, anonymity presented by cryptocurrencies makes it hard for authorities to track down offenders, later complicating the battle against cyber extortion [31]. To mention such concerns, future solutions should concentrate on leveraging emerging technologies like AI-driven cybersecurity systems which could diagnose and respond to threats in real time fast. Blockchain technology can have a role to develop data security and transparency. Governments and firms require to collaborate to launch stronger international regulations and unified cybersecurity standards to secure users and firms from blackmail. Finally, staying ahead of cybercriminals would need proactive strategy, integrating legal frameworks, public awareness, technological innovation.

- **Jurisdictional Issues:** Global cybercrime aspect complicates law enforcement attempts. Jurisdictional concerns provide essential concern to mention electronic blackmail, as cybercriminals sometimes operate over national borders, making that hard to use consistent legal architectures. Various countries have different rules associated with data protection, cybercrime, privacy that could complicate prosecuting offenders' process. Victims might tackle with searching for justice while perpetrators are placed in the other country with various legal systems/ while data is saved in several jurisdictions, making limitations for rule enforcement agencies to access evidence and take action [32]. Looking ahead, resolving jurisdictional

concerns would need developed international cooperation and unified global standards establishment for cybercrime legislation. Multilateral treaties and collaborative architectures, like those among rule enforcement agencies and international firms, would be critical to mention cross-border cybercrimes efficiently. Countries would require to adapt their legal systems to guarantee consistent cyber extortion rules' enforcement, streamline data-sharing protocols, develop capability to track and apprehend criminals who exploit jurisdictional gaps. Such collaboration would be key to struggle with global electronic blackmail aspect.

- **Human Factor:** Social engineering exploits human psychology, that is sometimes the poorest link in security systems. Factor of human remains one of the most considerable concerns to combat electronic blackmail. In spite of technology and cybersecurity developments, persons go on to fall victim to blackmail because of weak cyber threats awareness as well as unsecure online manners. A lot of people expose sensitive info via social media, engage in risky online interactions/fail to guarantee their digital devices accurately unknowingly. Such vulnerability is integrated by social engineering tactics, like phishing and manipulation that exploit human psychology to trick persons in showing private data/making compromising decisions [33]. Later, considering factor of human would need change to on-going education and awareness on cybersecurity. Public awareness campaigns and aimed training plans, especially for vulnerable groups such as teenagers and senior citizens, would be important in creating resilience in contrary to cyber extortion. Also, firms could perform cybersecurity culture plans for instilling safe online practices in workplace. Since cybercriminals growingly target human manner than only technical vulnerabilities, developing proactive strategy to online safety and fostering responsible digital treats would be key to decrease electronic blackmail risk.

6. Conclusion

Electronic blackmail refers to increasing threat exacerbated by new technologies. Decreasing the effect needs general strategy which integrates legal reforms, public awareness, technological safeguards. On-going research and collaboration between stakeholders are important to stay ahead of evolving cyber threats. So, cyber extortion is identified as one of the important cybersecurity concerns in new world, that has achieved better dimensions and complexity with digital technologies development. Different threats' kinds such as phishing, sextortion, ransomware illustrate that cybercriminals are constantly adapting their techniques to novel technologies. Simultaneously, such alike new technologies, like AI, developed cryptography, blockchain present robust means for recognizing, preventing, countering such threats. So, general strategy which contains increasing user awareness, developing security policies, using novel technologies could have efficient role in decreasing risks posed by cyber extortion. Finally, cooperation among technology firms, governments, customers in making safer cyberspace is important and crucial.

References

1. Zaltina P, Nurtjahyo LI. Right To Be Forgotten as a Legal Protection for The Victims of Electronic Sexual Violence Cases. The Indonesian Journal of Socio-Legal Studies. 2024;3(2):4.
2. AlGhanboosi B, Ali S, Tarhini A. Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. Computers in Human Behavior. 2023 Jul 1;144:107702.
3. Zolfagharipour L, Kadhim MH, Mandeel TH. Enhance the Security of Access to IoT-based Equipment in Fog. In2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT) 2023 Jul 4 (pp. 142-146). IEEE.
4. Ibrahim E, Sharif H, Aboelazm KS. Legal Confrontation of the Cyber Blackmail: a Comparative Study. Journal of Lifestyle and SDGs Review. 2025 Jan 17;5(2):e04039-.

5. Wang F. Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. International Review of Victimology. 2025 Jan;31(1):91-116.
6. Fisher T, Pieri Z, Howell CJ, O'Malley R, Tremblay L, Dawood M. Vendor Communication Themes in Darknet Ransomware-as-a-Service (RaaS) Advertisements. Computers in Human Behavior. 2025 Jan 17:108571.
7. Birthriya SK, Ahlawat P, Jain AK. Detection and Prevention of Spear Phishing Attacks: A Comprehensive Survey. Computers & Security. 2025 Jan 6:104317.
8. Mulligan C, Morsfield S, Cheikosman E. Blockchain for sustainability: A systematic literature review for policy impact. Telecommunications Policy. 2024 Mar 1;48(2):102676.
9. Ozkan-Okay M, Akin E, Aslan Ö, Kosunalp S, Iliev T, Stoyanov I, Beloev I. A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEe Access. 2024 Jan 18;12:12229-56.
10. Sonko S, Ibekwe KI, Ilojianya VI, Etukudoh EA, Fabuyide A. Quantum cryptography and US digital security: a comprehensive review: investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security. Computer Science & IT Research Journal. 2024 Feb 18;5(2):390-414.
11. Jubur M, Shrestha P, Saxena N. An In-Depth Analysis of Password Managers and Two-Factor Authentication Tools. ACM Computing Surveys. 2025.
12. Udeh CA, Orieno OH, Daraojimba OD, Ndubuisi NL, Oriekhoe OI. Big data analytics: a review of its transformative role in modern business intelligence. Computer Science & IT Research Journal. 2024 Jan 15;5(1):219-36.
13. Akinade AO, Adepoju PA, Ige AB, Afolabi AI. Cloud security challenges and solutions: A review of current best practices. Int J Multidiscip Res Growth Eval. 2025 Jan;6(1):26-35.
14. Al Habsi A, Butler M, Percy A, Sezer S. Blackmail on social media: what do we know and what remains unknown?. Security Journal. 2021 Sep;34:525-40.
15. Kainz O, Kissi S, Michalko M, Murin M, Nováková I, Šimko E. A Simulated Reconnaissance Attack on a Mobile Device. In2024 International Conference on Emerging eLearning Technologies and Applications (ICETA) 2024 Oct 24 (pp. 262-268). IEEE.
16. Gupta RK, Lamkuche HS, Prasad S. Enhancing the Security of Sensitive Data in Cloud Using Enhanced Cryptographic Scheme. InArtificial Intelligence-Augmented Digital Twins: Transforming Industrial Operations for Innovation and Sustainability 2024 Jan 20 (pp. 387-399). Cham: Springer Nature Switzerland.
17. Carletti R, Luo X, Adelopo I. Understanding criminogenic features: case studies of cryptocurrencies-based financial crimes. Journal of Financial Crime. 2024 Dec 24.
18. Syahreen M, Hafizah N, Maarop N, Maslinan M. A Systematic Review on Multi-Factor Authentication Framework. International Journal of Advanced Computer Science & Applications. 2024 May 1;15(5).
19. Ahmed M, Gaber M. An investigation on cyber espionage ecosystem. Journal of Cyber Security Technology. 2024 Sep 22:1-25.
20. Ananthakrishna V, Yadav CS. Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability. Nanotechnology Perceptions. 2024 May 5:560-77.

21. Ahmead M, El Sharif N, Abuiram I. Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. Crime Science. 2024 Oct 10;13(1):29.
22. Chapagain D, Kshetri N, Sihag VK. webCyberBlock: Cybersecurity and Cyber Ethics via Blockchain Technology–Need for Web Security, Software Practices, and End-User Cyber Education. InBlockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures 2025 (pp. 123-138). CRC Press.
23. Alamprese JA. Adult learning and education in digital environments: Learning from global efforts to promote digital literacy and basic skills of vulnerable populations. Adult Learning. 2024 May;35(2):73-81.
24. Kareem A, Akhtar MS, Tarar MA, Karim MA, Lighari M, Fatima K. Perceptions of Senior Citizens Regarding the Social Media Impact on Relationship between Parents and Teenagers: A Sociological Case Study in Dera Ghazi Khan. The Critical Review of Social Sciences Studies. 2024 Oct 24;2(2):339-59.
25. Hussein S, Mohammed S. Analyzing the Legal Framework and Implications of Federal Decree-Law No. 34/2021 in Combatting Cyber Blackmail in the UAE. In2024 2nd International Conference on Cyber Resilience (ICCR) 2024 Feb 26 (pp. 1-6). IEEE.
26. Al-Kasassbeh FY, Rukba RO, Abunaseir MH. Electronic Sexual Extortion in International Legislation and National Applications. International Journal of Criminal Justice Sciences. 2024 Jun 5;19(1):205-27.
27. Xu H. The positioning of China's anti-corruption agencies: law enforcement or political?. Crime, Law and Social Change. 2025 Jun;83(1):4.
28. Oladinni A, Odumuwagun OO. Enhancing Cybersecurity in FinTech: Safeguarding Financial Data Against Evolving Threats and Vulnerabilities.
29. Ravichandran R, Singh S, Sasikala P. Exploring School Teachers' Cyber Security Awareness, Experiences, and Practices in the Digital Age. Journal of Cybersecurity Education, Research and Practice. 2025 Jan;2025(1):1.
30. Kalinaki K. Ransomware Threat Mitigation Strategies for Protecting Critical Infrastructure Assets. InRansomware Evolution 2025 (pp. 120-143). CRC Press.
31. Coccia M. Converging Artificial Intelligence and Quantum Technologies: Accelerated Growth Effects in Technological Evolution. Technologies. 2024 May 10;12(5):66.
32. Magableh HY, Ahmad Al-Shawabkeh BK. The Problem of Jurisdictional Conflict and the Applicable Law on Cybercrime. Pakistan Journal of Criminology. 2024 Jul 1;16(3).
33. Dupont B, Fortin F, Leukfeldt R. Broadening our understanding of cybercrime and its evolution. Journal of Crime and Justice. 2024 Mar 1:1-5.