International Journal of Law and Societal Studies

DOI: 10.61424/ijlss
Journal Homepage: www.bluemarkpublishers.com/index.php/IJLSS

IJLSS
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Romance Scamming: Uncovering the Transnational Crime and Legal Challenges

Fazle Rabby[1] ✉ and Mohammad Moin Uddin Chowdory[2]
[12]Department of Law, University of Rajshahi, Rajshahi, Bangladesh.
Corresponding Author: Fazle Rabby, **E-mail**: fazlerabby365@gmail.com

| ABSTRACT

Romance scams have eventually become a major social and financial problem in Bangladesh as the frequency of victims of false online relationships rises daily. This present study aims to explain the nature and reasons behind romance scams, the consequences of this trend on society, and transnational crime and legal challenges. Three important groups, other people, fraudsters, and the police, were sought for insights using semi-structured interviews under a qualitative study methodology. Using thematic analysis of the gathered data for the study, the authors provide readers with a comprehensive understanding of why individuals participate in romantic scams, what goes through the minds of victims, and why it is difficult to capture the criminals, let alone convict them. Most importantly, the study highlights the absence of enough knowledge, legislative uncertainty, and ineffective tools to handle romance scams in Bangladesh. The research results offer some helpful knowledge about issues emerging from this crime and possible solutions for them.

| KEYWORDS

Romance Scam, Transnational Crime, Law Enforcement, Legal Challenges

| ARTICLE INFORMATION

ACCEPTED: 11 October 2024 **PUBLISHED:** 28 November 2024 **DOI:** 10.61424/ijlss.v1.i1.134

1. Introduction

These days, Bangladesh is seeing rising new and concerning patterns of crimes, including romance scams. This type of crime has seen attackers approach victims and engage them in a relationship that is emotionally and financially taxing, in contrast to more traditional types of cybercrime when the victim sends the offender an initial communication[28]. Target's recent spectacular growth, fuelled by easier access to the internet and social media, has given outlaws a chance to prey on weak people looking for company or who are looking for a life partner. While authorities are working to stop such cybercrimes, the elements defining internet interactions and the strategy used by fraudsters complicate matters. In the digital era, romance scams have become a widespread and detrimental form of transnational crime, preying on the vulnerabilities of individuals in search of friendship and affection. The international characteristics of romance scams hinder efforts to eradicate them. Fraudsters frequently operate from nations distinct from their victims, employing international communication networks and banking systems to conceal their activities.[7]

[7] Bidgoli, M. (2021). If You See Something Suspicious Online, Report It: An Investigation into Addressing and Overcoming the Challenges in Cybercrime Reporting. The Pennsylvania State University.

[28] Grispos, G. (2021). Criminals: Cybercriminals. In Encyclopedia of Security and Emergency Management (pp. 84-89). Cham: Springer International Publishing.

The geographical division presents considerable difficulties for law enforcement authorities, which must manoeuvre between diverse legal jurisdictions and collaborate with international counterparts to locate and apprehend offenders[27]. In 2013, the government of Bangladesh set up a Cyber Crime Tribunal to control cybercrime and handle connected matters. The tribunal lowers cybercrime at its heart and punishes the miscreants under the laws, which include the Information and Communication Technology Act of 2006, the Digital Security Act of 2018, the Cyber Security Act of 2023, and The Telecommunication Act of 2001. The cases related to cybercrime point to the causes of these activities, and the offenders face penalties according to these laws.

Romance scammers are a kind of confidence crime where they prey on victims and create a love relationship in order to either defraud them or obtain primary caregiver money or identity information[4]. Growing evidence from all around the world indicates that "traditional" online relationship scams are on the rise and are getting increasingly complex, so supporting more recent research findings that romance scams have lately become a major issue within Bangladesh [34]. Such frauds generate extreme psychological pain for the victims as well as other tangible costs for the people involved. According to Coluccia et al.[20], victims of romance scams typically feel humiliated, guilty, and embarrassed, so they do not disclose the instances or seek help. This psychological impact simply emphasizes the need for more intense prevention of such crimes.

Recently, in Bangladesh, particularly with the unchecked expansion of social networking sites and the internet, this kind of fraud has become rather common[6]. Online fraudsters create false profiles under the pretext of conning victims into either apparent love or sexual desire, so they get to steal from them and scam them, and also get to steal their identity[2]. Many people suffering major financial loss and mental stress, including shame, remorse, and social alienation, are victims of cybercrime [39]. Bangladesh's present legal and police systems are unable to identify how newly developing con artist tendencies behave. Many people avoid seeking aid or reporting embarrassing incidents due to humiliation; the general public is ignorant of the current risks presented by romance scams[2]. This makes it practically difficult to punish them; hence, there is a need for a multi-sectorial strategy embracing technology developments, penalties, and instructional programs[3].

[2]Ahmed, S. R. (2020). Identity Crime Framework and Model: Five Components of Identity Crime and the Different Illegal Methods of Acquiring and Using Identity Information and Documents. In Preventing Identity Crime: Identity Theft and Identity Fraud (pp. 46-186). Brill Nijhoff.

[3]Amirkhani, S., Alizadeh, F., Randall, D., & Stevens, G. (2024, May). Beyond Dollars: Unveiling the Deeper Layers of Online Romance Scams Introducing "Body Scam". In Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (pp. 1-6).

[4]Andonellis, M. (2022). Putting Your Heart and Wallet on the Line: How to Combat Romance Scams Targeting the Elderly. Elder LJ, 30, 135.

[6]Babu, K. E. K., & Siddik, M. A. B. (2022). Cybercrime in the social media of Bangladesh: an analysis of existing legal frameworks. International Journal of Electronic Security and Digital Forensics, 14(1), 1-18.

[20]Coluccia, A., Pozza, A., Ferretti, F., Masti, A., & Gualtieri, G. (2020). Online Romance Scams: relational dynamics and psychological characteristics of the victim and scammers. A scoping review. Clinical Practice and Epidemiology in Mental Health, 16(1), 24-35.

[27]Goni, O. (2022). Cyber crime and its classification. Int. J. of Electronics Engineering and Applications, 10(1), 17.

[34]Muhammud, F. S., & Muhammad, H. (2022). Cybercrime through love scams: What women should know?. Journal of Contemporary Islamic Studies, 8(2), 41-54.

[39]Rahman, D. A. M., & Islam, S. (2022). Financial and Social Costs Perspective Impacts of Cybercrime in the UAE: Policy-Guidance Addressing the Problem in Piecemeal Approach. SSRN.

Some believe that awareness campaigns, improved cyber law execution, international cooperation, and other measures taken against romance scams in Bangladesh help fight against them. The main issues, nevertheless, are fast changes in the scamming tools and materials as well as online openness[22]. Based on our work, this study identifies several significant legal issues in combating romance fraud. These are differences in legal provisions and

sanctions regarding internet fraud challenges in determining sovereignty and the process of apprehending an offender's extradition [10]. Some researchers suggest that a four-pronged approach comprising public awareness campaigns creative technologies, legal measures, and technological use will help to best tackle the issue [24]. This study aims to provide a preliminary understanding of the subject of romance scamming in Bangladesh to address what it is, how it started, and its consequences on individuals it targets, as well as the challenges the authorities experience in trying to stop this practice.

2. Literature review

2.1 Transnational Nature of Romance Scams

The crimes also include various related forms of fraud, particularly romance scams—also known as online dating frauds—which have become rather popular worldwide, including in Bangladesh. Usually resulting in a demand for money or sensitive information, these scams entail the offender creating a persona on the internet with the intention of fooling the victim into the growth of a romantic relationship with them. Chukwuka[19] mentioned that there is always room for such frauds to flourish, given the rising use of the internet and social media. It is still a serious problem since the con artist hides online, allowing the target clientele to be misled and taken into account, considering a large market[18].

However, transnational romance scamming activities between Bangladesh and the United States or Canada have become a significant concern. Fraudsters primarily employ social engineering and digital devices to defraud their vulnerable targets who are seeking a romantic partnership[23]. They create fabricated profiles on dating sites or social media platforms and, by utilizing VPNs and proxies, deceive you into believing that they are in your vicinity. This group of fraudsters invests time and engages in numerous messages, phone conversations, and even personal data sharing. Those who commit fraud frequently include information regarding their personal circumstances and travel expenses, and they require their victims to submit money in identifiable forms[25]. Scammers need a lot of time to build trust and make the victim feel like close friends; subsequently, they want money for some kind of promise, investment, or emergency.

[10]Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.
[18]Chuang, J. Y. (2021). Romance scams: Romantic imagery and transcranial direct current stimulation. *Frontiers in psychiatry*, *12*, 738874.
[19]Chukwuka, O. U. (2022). Internet fraud: the menace of 'yahoo boys'and the deceitfulness of riches. *Sapientia Global Journal of Arts, Humanities and Development Studies*, *5*(2).
[22]Dickerson, S., Apeh, E., & Ollis, G. (2020, November). Contextualised cyber security awareness approach for online romance fraud. In 2020 7th International Conference on Behavioural and Social Computing (BESC) (pp. 1-6). IEEE.
[23]Dickinson, T., & Wang, F. (2024). Neutralizations, Altercasting, and Online Romance Fraud Victimizations. *Deviant Behavior*, *45*(5), 736-751.
[24]Diega, G. N. (2022). Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies.
[25]Eseadi, C., Ogbonna, C. S., Otu, M. S., & Ede, M. O. (2021). Hello pretty, hello handsome!: Exploring the menace of online dating and romance scam in Africa. In *Crime, Mental Health and the Criminal Justice System in Africa: A Psycho-Criminological Perspective* (pp. 63-87). Cham: Springer International Publishing.

The emotional manipulation involved makes it somewhat easy for victims to overlook the lies, causing significant financial and emotional losses. These frauds are more complex, and those involved in such operations use different tactics to present attractive online personalities[40]. Many of them use fake images and false jobs and, most of the time, create histories for their accounts to be developed. Other techniques, such as "copycat," are among the techniques by which imitation of the target's interests and values strengthens the trust of the fraudster. Moreover, public use of protected communication mobile apps has enabled cybercriminals' freedom to get in touch with their targets without being closely watched by law enforcement authorities[15].

These patterns imply that fraudsters are building increasingly sophisticated networks and perhaps using artificial intelligence for some of their operations. They claim that by means of this technological development; they can handle several victims at once, therefore expanding the pool of potential victims from which to profit[10]. Romantic scams have terrible consequences since they financially compromise every victim by means of extortion of large sums of money[14]. Many cases go unreported, and there is absolutely no way to ascertain the actual scope of the

problem since some of the victims neglect to report scams because they feel ashamed or they do not want to be outcasts[1]. Public awareness, police actions, and international agency cooperation constitute the suitable means of combating romance scams in Bangladesh.

2.2 Types of Romance Scamming

Romance scams are relatively popular in the present world since the perpetrators use social platforms to carry out their evil deeds in the disguise of browsing for romantic or friendship relationships. Basically, their modus operandi starts with them creating fake identities on the most visited dating sites or online social networks. There are several types of romance scams, and each of them focuses on different aspects of trust and weakness in human character. Here are some of the most common types:

2.2.1 Classic Romance Scam

In a common type of romance scam, the perpetrator will create a fake profile for themselves on online dating sites or social networks. They gain the victim's trust over time and work closely with the victim as they help them out. After gaining the victim's trust and emotional attachment, the scammer creates an emergency that needs to be solved through financial capital[1]. They may seek cash to cover hospital costs, airline tickets, and other emergency circumstances. A scam persists where the scammer is able to defraud cash from the victim[8]. Sometimes, the offender engages in acts like making the target have feelings towards him or her so that they may threaten the victim's partner to send money more quickly. People are often threatened and compelled to give personal details or more money for the purpose of consolidating what the scammers have told the victim is a relationship.

[1]Agina, E. M. (2022). Efficacy of the Cyber Security Legal Framework in Addressing Cybercrime: A Focus on Kenya (Doctoral dissertation, University of Nairobi).
[8]Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. International Review of Victimology, 02697580241282782.
[10]Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55.
[14]Carter, E. (2024). The Language of Romance Crimes: Interactions of Love, Money, and Threat. Cambridge University Press.
[15]Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen Co-production of cyber security: Self-help, vigilantes, and cybercrime. Regulation & Governance, 12(1), 101-114.
[40]Rege, A., & Bleiman, R. (2020, June). Ransomware attacks against critical infrastructure. In *Proc. 20th Eur. Conf. Cyber Warfare Security* (p. 324).

2.2.2 Online Dating Scams

In these scams, fake identities come up with fake profiles on websites for dating or escort services, with pretensions to provide dating or paid companionship services. They may ask for upfront payments for the meetings and, in the process, use fake pictures and stories. When the payment is made, the scammer disappears without having offered the promised services to the victim[26]. In this process, scammers may spend quite some time chatting with them and even come up with fake life events to blend. They can also use fake verification images or videos to make the victim believe the truth about the stranger.

2.2.3 Heritage Frauds and Financial Investment Frauds

In this romance scam, swindlers make people believe they are owed a significant amount of money or have a high-paying business deal they want to offer. They may say they require a little push to enable them to get the money or with an investment promising to offer some amount of money to the victim[23]. They convince the victim that they will return the money back once they have secured something. Sometimes, these people come up with good stories and even dizzying legal documents that make the whole process seem to be genuine. Once, the victims are coerced into paying many times, each and every time under a different pretext of surmounting other barriers to access the presumed money.

2.2.4 Gift Card Scams

In these scams, after building a relationship, scammers ask the victim to send gift cards for various reasons, like they need a phone to communicate, they have to travel, or the cards for them to show how they feel. Gift cards are preferred for use, restocked, or cashed since the transactions can easily go unnoticed[43]. Hackers and scammers

engage the victims in feeling guilty or pressured to meet the demands of such requests. The unsuspecting victim is left drained monetarily and emotionally, and by the time the scammer receives the gift cards received and redeemed almost instantly.

2.2.5 Travel and Vacation Scams

Online scammers pretend to plan a visit to see the victim, but then they experience some sort of mishap that requires them to pay some amount of money, such as visas, tickets, or accommodation, amongst other things. They compel the victim to bear such costs, assuring that they will be reimbursed as soon as they get there. After this, the scammer will continue to ask for more money for more 'issues' or will simply disappear[35]. These scammers develop various tactics of pressure and emotions so the victim does not doubt the identity of the offender and believes that they will soon meet. It is much the same with each new request for money as those who defraud others promise, and this is the final straw needed to get over the hump, but with fake emergencies going as long as the victim will keep sending money.

[23]Dickinson, T., & Wang, F. (2024). Neutralizations, Altercasting, and Online Romance Fraud Victimizations. Deviant Behavior, 45(5), 736-751.
[26]Gil, B.D., & Zeng, Y. (2022). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. Journal of Financial Crime, 29(2), 460-475.
[43]Tomas, F., & Zanden, T. (2023). There Are Layers to Liars: A Systematic Literature Review of Online Dating Deception.
[35]Paat, Y. F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Social Work in Mental Health, 19(1), 18-40.

2.3 Psychological and Financial Impact on Victims

Emotionally, the results of such frauds may be terrible, but financially, they could be disastrous as well. Depending on the fraudster, they could be able to take big amounts of money from their victims, which would cause debt and destitution. People also lose their sources of income, their vehicles, homes, and so on; the lost money is not only the actual money thrown away and having to survive by only wages and salaries. Payne and Hadzhidimova [37] claim that the financial consequences can be disastrous, so the sufferers might need time to achieve financial recovery. Financial stress adds to the psychological stress, which in turn can simply lead to a cycle of tension and worry regarding the money lost from the scams, which corresponds not only with the monetary loss from the scams but also continuously in the life of the victims. For example, individuals can find it difficult to get loans or credit in the future—a definite path via financial preparation. Older victims, as it would be evident, depend on smaller fixed incomes or retirement benefits; thus, they may take more time to recover in case they are targeted. Besides, financial compromise increases vulnerability and helplessness, therefore aggravating the psychological effect[11]. Furthermore, entwined with each other and having major detrimental consequences on victims are psychological and economic aspects. Such strain leads to negative mental states, the worst of which include mental diseases, which are subsequently exacerbated by financial loss and so influence physical health.

2.4 Challenges in Legal and Law Enforcement Responses

Apart from financial loss, it was discovered that victims of romance fraud suffer notable emotional and psychological effects[44]. Many people feel ashamed and betrayed, so they do not seek the offender for the harm they have committed to them. Khan[30] clarifies that victims suffer certain psychological negative effects in addition to physical damage, emphasizing the need for help in standing another trial. Another significant impact a victim may have is a financial loss; occasionally they are even cleared dry, both materially and emotionally as well [40].

As the victim falls into the trap of romance scams, it can have a quite negative psychological and emotional effect. Rather, the victims who are emotionally close to the frauds believe they have discovered their boyfriend and spouse. Anxiety, depression, or even Post-traumatic stress disorder (PTSD) could be among the repercussions. Taking anything that causes drug misuse means that these emotional effects could hinder their capacity to trust other individuals, thereby isolating them socially. Few victims can understand how they have been duped, so more often, there is shame and self-blaming. For some of the stigmas society, victims aggravate this deep emotional pain, so these victims will hardly seek law enforcement assistance or report the crime. Likewise, Khan [30] notes that psychological distress is sometimes disregarded when it comes to pain or anguish connected to such scams.

Therefore, victims must be in a position to welcome counselling sessions and even other victims to help in the evaluation of this product since they equally need to accept their self-value.

[11]Bruhn, A. G. (2015). Personal and social impacts of significant financial loss. Australian Journal of Management, 40(3), 459-477.
[30]Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. Laws, 13(4), 44.
[37]Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. International Journal of Cyber Criminology, 14(1), 81-105.
[40]Rege, A., & Bleiman, R. (2020, June). Ransomware attacks against critical infrastructure. In Proc. 20th Eur. Conf. Cyber Warfare Security (p. 324).
[44]Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. Criminology & Criminal Justice, 16(2), 176-194.

Although romantic scams are on rise, Bangladesh's legal and law enforcement systems have several shortcomings. Authorities almost cannot control the operations of the scammers since their tactics are always changing and almost impossible to grasp[45]. Legal responses are less effective as most of these crimes are carried out internationally, and the internet provides anonymity. Strengthening of cyber law implementation and international cooperation should be focused as the best ways to fight romantic scams successfully [2]. Chowdhury & Fahim[17] fighting the so-called romance scams also presents another significant challenge since it entails intricate and always changing methods of deception. Law enforcement authorities find it quite challenging to stay up as criminals mostly change their operations to include new technologies and trends. Since they can quickly create accounts from anywhere, scammers utilize false identities, encryption, and social engineering to prevent easy tracking. The present laws in Bangladesh can only be characterized as being in a growth phase, with the nation's legal system far from efficient in adjusting to cybercrime because romance scams combine elements of emotional and financial exploitation.

Furthermore, it is more difficult because most of the cases feature international aspects. Often involved in cross-border frauds, criminals prey on people from many nations. Usually lacking is this global quality that calls for strong transnational cooperation. Obstacles in catching and presenting the scammers include inaccessibility of legislation and regional restrictions. Although joint intervention is desired and cooperation and information sharing are needed, it is not easy to accomplish. Chowdhury and Fahim[17] discuss how Bangladesh law enforcement authorities may not have sufficient training in handling cybercrime and could occasionally be inadequately equipped. Along with sophisticated tools to solve and stop scams occurring in cyberspace, cybercrime teams require training. Law enforcement also has to alert potential victims of the hazards and possible dangers related to such frauds; this kind of operation also requires financing and constant effort.

Another is related to the insufficient development of present cyber laws. Though Bangladesh is making great progress toward computer crime laws, permanent change is needed to handle new forms of cybercrime [38]. The quickly expanding cyberspace environment makes the legal rules on a digital plane dynamic. In conclusion, it is important to underline that only an integrated approach implies the following activities—adjustments in legal regulation, an increase in the effectiveness of law enforcement practice, and the development of international cooperation in the sphere.

[2]Ahmed, S. R. (2020). Identity Crime Framework and Model: Five Components of Identity Crime and the Different Illegal Methods of Acquiring and Using Identity Information and Documents. In Preventing Identity Crime: Identity Theft and Identity Fraud (pp. 46-186). Brill Nijhoff.
[17]Chowdhury, M. A. A., & Fahim, M. H. K. (2020). An Insight Into The Cybercrimes And Cyber Security Measures In Bangladesh: Quest For Operative Legal Remedies. Solid State Technology, 63(6), 22453-22468.
[38]Rahaman, M. M. (2022). Recent advancement of cyber security: Challenges and future trends in Bangladesh. Saudi Journal of Engineering and Technology, 7(6), 278-289.
[45]Yesmen, N., & Ahmed, N. (2022). The nature and challenges of cyber policing: A study on criminal investigation department (cid), dhaka, bangladesh. Asian Journal of Sociological Research, 210-214.

2.5 Public Awareness and Education

One of the best strategies to offset the consequences of fraud is raising public awareness. If one is aware of elements of the scams and susceptibility factors, one can avoid falling victim to them [44]. Public efforts must continue to empower possible victims to be informed of the risks presented by online relationships and common scam techniques. More importantly, currently, the understanding regarding these concerns [in Bangladesh] is minimal, so there is a need to establish more effective education and awareness-raising programs. The foundation of successful campaigns should consist of several aspects. First of all, they should let people know about typical situations and what kind of indicators—including asking for money, claiming to be in love after a brief period of knowing someone, and providing lots of different details [16]. By introducing such indicators to people, one can make sure the latter would not fall victim to these frauds.

Another crucial consideration is lighting on the fact that the primary goal of the scammers is to evoke sensitive emotions in the victims. When looking for a connection online, people might avoid falling for these fake people by being aware of the emotional angles that affect people want to pursue [44]. This covers knowledge of psychological techniques, including victim seclusion, fear-mongering with simulated crises, and love bombing. More so, awareness-raising campaigns should take into account other elements of society and culture that expose people to become victims of bogus romance fraud [13]. People in Bangladesh depend on these features of fraud since they feel under pressure in terms of marriage and relationships.

As indicated, the educational campaigns have to offer the subjects the necessary frameworks where particular hazards occur and culturally acceptable advice [41]. Taking education to the masses calls for applying as many strategies to guarantee optimum impact. Along with general informational efforts, this includes focused professional development for certain populations at risk—including the elderly and those who do not effectively use information technologies. Online programs, classroom, or workshop lessons can assist one in learning the finest approaches for properly managing and running online connections [31]. Furthermore, campaigns should clarify that falling for clever strategies does not make one stupid; rather, it indicates that one fell for fraud. Encouragement of free, reasonably anonymous reporting eliminates stigma from the equation, therefore enabling those who have fallen for fraud to come forward. For those who believe they are being harassed, general internet forums and phone helplines might offer quick assistance.

[44]Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. Criminology & Criminal Justice, 16(2), 176-194.

[16]Chethiyar, S. D. M., Vedamanikam, M., & Sameem, M. A. M. (2021). Losing The War Against Money Mule Recruitment: Persuasive Technique In Romance Scam. Ilkogretim Online, 20(3), 2569-2585.

[13]Carter, E. (2021). Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. The British Journal of Criminology, 61(2), 283-302.

[31]Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. International Journal of Cyber Criminology, 9(2), 205.

[41]Rehman, S., & Manickam, S. (2023). Towards a Cybersecurity Awareness Program for Non-Technical Audiences in Malaysia. In Cybersecurity for Decision Makers (pp. 85-97). CRC Press.

2.6 Technological Solutions and Preventive Measures

Fighting romance fraud mostly depends on technology. Methods including artificial intelligence (AI) and machine learning can help spot possible frauds on social media and dating sites, triggering a system red alert. More effective protection should be developed, and reporting processes should be streamlined as much as feasible to enable individuals to more freely report such scams [40]. Governments, law enforcement, and tech businesses should collaborate on comprehensive methods to tackle these scams. Ensuring people report any seen irregularity in the shortest time possible mostly depends on organizational accommodating reporting systems. Such systems should be easily accessible and connected to dating services, social networks, and other pertinent websites. This makes visitors submit important data to the site that can enhance the detection algorithms and simplify reporting [33]. Moreover, giving the scam-reports user comments helps to reassure individuals that they belong inside the platform's safety. Correct identity identification and other higher-level authentication using any device more than one for the same account can help to significantly reduce these scams [29]. The methods involving several phases of user authentication run the risk of locking out scammers since they cannot create phony identities several times.

Because of regular audits and security detail modification required in combating the always-changing frauds, these policies are strong against new ones.

Particularly in police departments and legislators, there is a need for coordinated efforts supported by other technology corporations as well as public and non-governmental organizations. Technical companies can supply prosecutors and investigators with data and case analysis on several issues. Legislation must be passed to empower such efforts and force the platform owners to guarantee sufficient security systems have been implemented and in circumstances where their fraud-connected activities are imminent, notify the same [42]. The situation is significant as even the most ordinary frauds, including romance scams, could arise online and include several states. To establish the best practices for other nations about the handling of transnational crime inquiries, they must work together. Cooperation between public and private businesses seems to assist in creating fresh approaches to prevent fraud in government operations. For instance, certain governments can provide financing for such initiatives, while some IT corporations can collaborate with cybersecurity companies to create improved detection technology.

3. Research Methodology

3.1 Research Design

This study will use qualitative methods to gain a thorough understanding of romance scamming as a recently emerging issue in Bangladesh. Qualitative research is chosen for its capacity to investigate social issues via the nature, experiences, views, and behaviour of people [21]. If the researcher is to grasp the causes of the crime as well as examine stakeholders' positions, qualitative research methods give flexibility.

[21]Creswell, J. W., & Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage publications.
[29]Jong, K. (2019). Detecting the online romance scam: Recognising images used in fraudulent dating profiles (Master's thesis, University of Twente).
[33]McCoy, D., Park, Y., Shi, E., & Jakobsson, M. (2016). Identifying scams and trends. Understanding social engineering based scams, 7-19.
[40]Rege, A., & Bleiman, R. (2020, June). Ransomware attacks against critical infrastructure. In Proc. 20th Eur. Conf. Cyber Warfare Security (p. 324).
[42]Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. Journal of Accounting & Organizational Change, 17(2), 164-196.

3.2 Data Collection

Semi-structured interviews will be the primary method of data collection for the present study. It will give the researcher a chance to get answers clearly and express some of the subjects the researcher raises via questions. The questions will, however, not be asked in exactly the same sequence or language and allow room to augment the interview depending on the responses of the participants. This kind of organization enables one to genuinely explore the particular elements that might show up during the interview and strengthen the body of information [12].

3.3 Sampling

Based on the present research, recommendations of people suitable to provide information about romantic scamming will be made using a purposive sample method [36]. Three main groups will form the sample:

Mass Public: This study intends to investigate the statistical data of those becoming victims of romance scams.

People engaged in a romance scam: Every one of those engaged—directly or indirectly—in the execution of this crime will be questioned about their motives, methods, and relationships. Using this group one could have to coordinate with the police department among other authorities.

Authorities pertaining to Law Enforcement: The extent of the problem, challenges in tracking down and arresting criminals as well as the current methods in handling the crime will be understood with the help of law enforcement officials and investigators engaged in cybercrime and financial fraud offenses.

3.4 Interview Process

Depending on the participant's convenience, the semi-structured interviews will be carried out either in person or remotely, say using Skype or Face-time. Depending on the quality of the response and participant stamina, each interview should normally last between thirty to sixty minutes. In order to type them accurately, participant interviews will lastly be videotaped depending on the participants' permission.

3.5 Ethical Considerations

Since romance scams are a topic intimately related to possible legal problems, strict ethical considerations will be followed. Potential participants will be fully informed of the goal of the study, sign a consent form to participate in the study, and be advised that they have the right to withdraw from the study at any moment. Should participants engage in fraud, their names will not be shared, so the study will be conducted anonymously and with confidentiality. The gathered data will be kept private and applied only for research purposes.

[12]Bryman, A. (2016). Social research methods. Oxford university press.

[36]Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and policy in mental health and mental health services research, 42, 533-544.

3.6 Data Analysis

After hand and literal transcription, the interview material will be examined. To find trends, themes, and categories of issues for the participants—their experiences and motivations will be taken into account.[9] With regard to sociology, psychology, and legal prospective, this approach will also let the researcher progress very significant knowledge of the multifarious character of romantic scamming in Bangladesh. Themes will then be synthesized to foster a general appreciation of the particular phenomenon.

This is qualitative research so the findings of this study could not be applicable to other members of the society. Furthermore, it is possible to see issues in gathering people directly connected to romance scams. The researcher plans to, wherever feasible, cooperate with police agencies and other community organizations in order to offset this. This investigation could contribute to acquiring a comprehensive perspective of romantic scamming in Bangladesh and produce insightful results to clarify the causes of such activity, its effects, and viable solutions.

4. Result

4.1 Demographic Information of Participants

The demographic profile of the respondents, such as gender, age, education level, marital status, occupation, income, nationality (origin), and purpose of visit and length of stay, are analysed with the frequency distribution and provided in the following tables. Table 4.1 depicts the descriptive statistics of the respondents' demographic factors (gender, age, marital status, occupation).

Table 4.1: Profile of the Respondents (Gender, Age, Marital Status, Occupation)

Variable	Descriptions	Frequency	Percentage
Gender	Male	38	76.0
	Female	12	24.0
	Total	50	100.0
Age	18-25	22	44.0
	26-33	18	36.0
	34-41	5	10.0
	42-49	4	8.0
	50 and above	1	2.0
	Total	50	100.0
Marital Status	Single	32	64.0
	Married	16	32.0

	Divorced	2	4.0
	Total	50	100.0
Occupation	Private Sector	2	4.0
	Students	12	24.0
	Public Service (Police)	10	20.0
	Unemployed	26	52.0
	Total	50	100.0

As shown in Table 4.1, the gender distribution is fairly balanced, with males comprising 76.0% and females 24.0% of the respondents. The majority of respondents, 44.0%, fall within the age group of 18-25 years old. This is followed by 36.0% in the 26-33 age group, 10.0% in the 34-41 age group, 8.0% in the 42-49 age group, and 2.0% who are in the 50 and above age group. Regarding marital status, the majority, 64.0%, are single, while 32.0% are married and 4.0% are divorced. Additionally, the occupation status of the respondents is as follows: 52.0% are unemployed, 24.0% are students, 20.0% are public service (police), and 4.0% are private sector job holders.

Table 4.2*:* Profile of the Respondents (Education Level, Income, Origin)

Variable	**Descriptions**	**Frequency**	**Percentage**
Education Level	Never been to school	2	4.0
	Primary school	11	22.0
	Secondary School	14	28.0
	Diploma	17	34.0
	Degree/Bachelor	5	10.0
	Masters	1	2.0
	Total	50	100.0
Income (BDT)	Less than 5000	3	6.0
	5001-10000	23	46.0
	10001-15000	13	26.0
	15001-20000	8	16.0
	20001-25000	2	4.0
	More than 25000	1	2.0
	Total	50	100.0

Table 4.2 shows the descriptive statistics of the respondents' demographic factors for education level and income (in Bangladeshi Taka), of the respondents. In terms of education level, the majority of the respondents have completed a diploma (34.0%), followed by secondary school (28.0%), primary school (22.0%), Degree/bachelor (10.0%), never been to school (4.0%), and master's (2.0%). Respondents were asked to provide information about their monthly income in Bangladeshi Taka (BDT). Most of the respondents have an income of about 5001 to 10000 BDT, which is 46.0%, followed by 10001-15000 BDT (26.0%), 15001 to 20000 BDT (16.0%), less than 500 BDT (6.0%), 20001 to 25000 BDT (4.0%), and more than 25000 BDT (2.0%). Besides, the actuality of romance scamming is not just some vagueness but a real enrolment in certain geographical spaces. In Bangladesh, certain parts of the country became famous for these kinds of illegitimate undertakings; a large number of the scammers belong to the Modhupur area in Tangail district and some areas in Gazipur and Dhaka.

4.2 Discussion

The legal, social, transnational, and technological effects of the rising incidence of romance scamming in Bangladesh have a number of implications for today's society. The procedures employed to address the aforementioned implications are crucial to mitigating these frauds and protecting those who could be susceptible to falling victim. The increased complexity of the romance scam requires improvement on the existing Bangladesh cybercrime legal framework. It is clear that current laws are insufficient, and they require enhancement with new

laws that will explain in detail what online dating fraud is and appropriate punishments for scammers. Proper legislation will serve its purpose of discouraging scammers and helping to convict such people. From the findings of this study, it is clear that gross awareness and more training are needed by law enforcement agencies while handling cases of romance scams. This also involves academics in areas like cyber criminality, investigation and case-making, digital forensics, and cross-border operations. Enhancing police capacity to detect, investigate, and prosecute fraudsters will help to control the incidences of these vices. [39] These data demonstrate that people from Bangladesh are also active in answering the scammer's call and that real, global efforts are necessary to curb the synthetic and nefarious nature of such schemes. The discussion can be framed around the following key areas:

Understanding the Scale and Impact: The first thing that must be done to address romance scamming, therefore, will be to establish the level of impact that it has yet caused on the affected persons. Research shows that there has been an increase in the number of such scams, and yet individuals lose their money and sometimes morale [39]. To make effective policies and utilize the resources, it is essential to collect the right information.

Strengthening Legal and Law Enforcement Frameworks: The current legal frameworks of Bangladesh must be reinforced to avoid the loopholes created due to the highly dynamic nature of romance scams. Among such measures, amendments to cybercrime legislation have been introduced aimed at introducing provisions covering online dating fraud and improving the capacities of law enforcement bodies in combating such crimes. International cooperation is also needed here as it refers to many scams which cross the national borders.

Raising Public Awareness: Community alerts form a critical component of combating romance scams. Awareness raised to the general public can prevent any likely victim from falling prey to con artists' tricks. It is therefore important for any effective campaign to use as many tools as possible which may include the use of social media [32]. Further, such organizations can intensify these efforts through cooperation with technology companies and social networks.

Implementing Technological Solutions: Detecting and preventing romance scams, technological developments should provide a promising technique for security as a whole. For instance, when using dating and social media sites, this can be checked by clean technologies and AI. Also, friendly structures where users can easily report can help the victims to report the scams early enough, and hence fast responses from the authorities will be made [40].

Providing Support to Victims: Some of the general measures that should be taken in combating the phenomenon of romance scams include setting up structures for the victims. Besides, through examinations and consultations from psychological experts and financial advisors, the victims recover from their experiences. A lack of support, embarrassment, or stigma associated with reporting such scams is also important when designing the environment in which victims can give their reports [30].

Therein, it is an integral conclusion that combating the phenomenon of romance scamming in Bangladesh is possible only in one way with an integrated approach. It is only when society adapts to the enormity of the problem; the improvement of legal systems; increases public awareness; utilizes other technological means; and gives the necessary assistance to individuals who become victimized by such scams, that one can diminish the effects of being scammed.

[30]Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. Laws, 13(4).

[32]Mahmud, S. R. (2020). The effectiveness of Facebook advertisements on purchase intention of customers in Malaysia. South Asian Journal of Social Sciences and Humanities, 1(1), 97-104.

[39]Rahman, D. A. M., & Islam, S. (2022). Financial and Social Costs Perspective Impacts of Cybercrime in the UAE: Policy-Guidance Addressing the Problem in Piecemeal Approach. SSRN.

[40]Rege, A., & Bleiman, R. (2020, June). Ransomware attacks against critical infrastructure. In Proc. 20th Eur. Conf. Cyber Warfare Security (p. 324).

4.3 Flaws and Recommendations for Law Enforcement in Bangladesh

The Cyber Security Act 2023, of Bangladesh, is to protect from cybercrimes and romance scams among other crimes. Section 24 of the act which deals with online fraud and scams makes it an illegal act. Specifically, under section 24 penalties are provided for deception labelled as "fraud by personation" such as scams evading individuals on online dating platforms. The punishment includes imprisonment for a term that may extend to five years, and also be punishable with a fine which may extend to 500 Thousand Bangladeshi Taka or both. The Act's penalties are meant to discourage romance crimes, but there are weaknesses when it comes to implementation as well as application of these penalties owing to probably structural and procedural inefficiencies [33]. Here are some of the prominent loopholes:

1. Lack of Clear Definitions and Scope: The CSA has certain definitions related to 'cyber fraud', 'identity fraud', and other related offenses which are rather nebulous, by design or otherwise, as can be appreciated. For instance, what is considered as "false or misleading information" is not very clear. It may result in some hitches and irregularities and can open up loopholes that pry embezzling individuals can seal.

2. Low Penalties and Absence of Repeat Offender Clauses: Although under CSA the penalties for cyber fraud and identity fraud are imposed, the Act has relatively lighter penalties compared to its earlier version the Digital Security Act. An important weakness is that there are no higher penalties for second-time offenders or repeat criminals, which may let regular cyber criminals operate without much more fear or consequences.

3. Overreliance on Law Enforcement without Specialized Training: Under the Act, the police is given open permission to investigate and arrest some cybercrime offenses on matters of likelihood. Nevertheless, since the current crop of officers lacks training in cyber forensics and digital crime investigation, they might find it very hard to work on intricate scams as they call for technological expertise.

4. Limited Victim Support and Awareness Initiatives: The CSA does not consist of rules for victim support services or awareness programs that have become important for people to detect, report, and reclaim via cyber scams.

6. Inadequate Infrastructure for Digital Crime Prevention: For good cybercrime legislation to work, it has to be backed by strong IT support like protected complaint handling systems, specialized cybercrime police departments, and big data analytical tools. Currently, these resources are scarce in Bangladesh, it becomes very difficult to handle and control the rising incidences of romance scams.

To address the loopholes and enhance the country's defences against romance scams, several actions can be taken:

1. Clarify Legal Definitions and Narrow the Scope: To avoid such broad interpretations, which subsequently lead to a 'two-faced' application, apparent clarification of the CSA called for more specific definitions of terms like 'cyber fraud' and 'identity fraud'. Well-defined terms assist law enforcement and judicial officials to work diligently by only increasing cases in court if they qualify for the law.

2. Introduce Stricter Penalties for Repeat Offenders: The provisions for increasing the severity of the punishments where the offense is repeated can have a lot of motivational impact on habitual cyber criminals. When the penalties for multiple offenses increase, then the law has the potential to greatly minimize instances of repeat offenses and thus discourage people from undertaking successive romance scams.

3. Enhance Law Enforcement Training: Presently, it is required to train officers involved in policing cyberspace, computer and crime investigations, and support to victims. Concerning the requirement established by Act 37 for training on risky and intricate scams as romance frauds can enable the officers understand and manage the security risk into the training scope.

[33]McCoy, D., Park, Y., Shi, E., & Jakobsson, M. (2016). Identifying scams and trends. Understanding social engineering based scams, 7-19.

4. Increase Victim Support and Public Awareness: To prevent citizens from being victims of romance scams releasing information to the general public of other countries about them is helpful. If services like telephone numbers or web platforms to report cases were available the victims would be willing to report the cases.

5. International Strategies to Combat Romance Scams: On prevention of romance scams internationally, various approaches can be applied successfully inclusive of cross-jurisdictional law enforcement cooperation, public education, and cooperation between governments and between technology companies. Improving public awareness, putting in place channels for reporting the fraudsters, and being helpful to the victims could all make transnational efforts to minimize these fraudulent schemes even better.

5. Conclusion

In Bangladesh, romance scamming has become a complex and ever-growing threat, as is evidenced by the transnational crime of online fraud. The advance of internet connectivity in homes and the social media craze have created fresh opportunities for scammers to defraud the public. It is also important to note that while victims are defrauded, they also receive severe emotional and psychological trauma; the depth of the problem, therefore, goes a notch higher. Under present-day laws and enforcement of justice, there are barriers that hinder the crippling of these scams, mainly as a result of the changing faces of the cons and the essence of the web as an environment for one cannot easily identify the other. As people change their communicational patterns in response to the pandemic, romance scams remain unsolvable problems in the sphere that require constant population information to prevent individuals from becoming victims of such scams. These scams have cost people of various countries a lot of money and produced losses for the entire nation. They have also allowed victims to experience things like mental distress, emotional distress, betrayal, and, where necessary, a loss of confidence.

6. Limitations and Future Work

The following analysis points to both the strengths and the weaknesses of this study, which have to be acknowledged. The amount of data is rather restricted, and the majority of information is gathered without employing primary data collection methods and making quantitative evaluations. This limited the study's scope as major primary data, such as interviews with victims, were not included. Interestingly, the use of quantitative data in subsequent studies may give broader insights into romance scams in Bangladesh. [39]

The recommendations for future research follow from the limitations encountered in undertaking this particular study. Controlling a large number of data-gathering activities, such as quantitative questionnaires and face-to-face interviews with the victims and police officers, would give a much better and broader insight into the nature of the specific type of scams described as romance scams. Thus, collecting such data would allow for performing more objective statistical analysis and recognizing more patterns and trends. Also, the inter-regional analytical comparisons may be helpful in investigating the scale of the international activity of the perpetrators and the distinctive characteristics influenced by various cultures, societies, and economies in different parts of the transnational to affect the outcomes of the romance scams.

Another a priori research domain is the ongoing identification of new types of scams and the creation of respective defences. Because scammers follow advancements in technology while devising their own tricks, ability and future research should be directed towards identifying the technological way of avoiding the scams, including artificial intelligence and machine learning systems. Successful delivery of these solutions will require innovative partnerships with technology companies and social media platforms. Last but not least, future research must examine the reactionary psychological and social effects of romance scams on its victims more comprehensively. - A further goal will be to explain the types of mental health impact as well as social relationship disturbance with a view of assisting victims to recover and learn how to stand firm in case they experience such an event again.

References

[1] Agina, E. M. (2022). *Efficacy of the Cyber Security Legal Framework in Addressing Cybercrime: A Focus on Kenya* (Doctoral dissertation, University of Nairobi).

[2] Ahmed, S. R. (2020). Identity Crime Framework and Model: Five Components of Identity Crime and the Different Illegal Methods of Acquiring and Using Identity Information and Documents. In *Preventing Identity Crime: Identity Theft and Identity Fraud* (pp. 46-186). Brill Nijhoff.

[3] Amirkhani, S., Alizadeh, F., Randall, D., & Stevens, G. (2024, May). Beyond Dollars: Unveiling the Deeper Layers of Online Romance Scams Introducing "Body Scam". In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

[4] Andonellis, M. (2022). Putting Your Heart and Wallet on the Line: How to Combat Romance Scams Targeting the Elderly. *Elder LJ*, *30*, 135.

[5] Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga*, *10*(38), 113-122.

[6] Babu, K. E. K., & Siddik, M. A. B. (2022). Cybercrime in the social media of Bangladesh: an analysis of existing legal frameworks. *International Journal of Electronic Security and Digital Forensics*, *14*(1), 1-18.

[7] Bidgoli, M. (2021). *If You See Something Suspicious Online, Report It: An Investigation into Addressing and Overcoming the Challenges in Cybercrime Reporting*. The Pennsylvania State University.

[8] Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, 02697580241282782.

[9] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, *3*(2), 77-101.

[10] Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

[11] Bruhn, A. G. (2015). Personal and social impacts of significant financial loss. *Australian Journal of Management*, *40*(3), 459-477.

[12] Bryman, A. (2016). *Social research methods*. Oxford university press.

[13] Carter, E. (2021). Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. *The British Journal of Criminology*, *61*(2), 283-302.

[14] Carter, E. (2024). *The Language of Romance Crimes: Interactions of Love, Money, and Threat*. Cambridge University Press.

[15] Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen Co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101-114.

[16] Chethiyar, S. D. M., Vedamanikam, M., & Sameem, M. A. M. (2021). Losing The War Against Money Mule Recruitment: Persuasive Technique In Romance Scam. *Ilkogretim Online*, *20*(3), 2569-2585.

[17] Chowdhury, M. A. A., & Fahim, M. H. K. (2020). An Insight Into The Cybercrimes And Cyber Security Measures In Bangladesh: Quest For Operative Legal Remedies. *Solid State Technology*, *63*(6), 22453-22468.

[18] Chuang, J. Y. (2021). Romance scams: Romantic imagery and transcranial direct current stimulation. *Frontiers in psychiatry*, *12*, 738874.

[19] Chukwuka, O. U. (2022). Internet fraud: the menace of 'yahoo boys'and the deceitfulness of riches. *Sapientia Global Journal of Arts, Humanities and Development Studies*, *5*(2).

[20] Coluccia, A., Pozza, A., Ferretti, F., Masti, A., & Gualtieri, G. (2020). Online Romance Scams: relational dynamics and psychological characteristics of the victim and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health*, *16*(1), 24-35.

[21] Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

[22] Dickerson, S., Apeh, E., & Ollis, G. (2020, November). Contextualised cyber security awareness approach for online romance fraud. In *2020 7th International Conference on Behavioural and Social Computing (BESC)* (pp. 1-6). IEEE.

[23] Dickinson, T., & Wang, F. (2024). Neutralizations, Altercasting, and Online Romance Fraud Victimizations. *Deviant Behavior*, *45*(5), 736-751.

[24] Diega, G. N. (2022). Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies.

[25] Eseadi, C., Ogbonna, C. S., Otu, M. S., & Ede, M. O. (2021). Hello pretty, hello handsome!: Exploring the menace of online dating and romance scam in Africa. In *Crime, Mental Health and the Criminal Justice System in Africa: A Psycho-Criminological Perspective* (pp. 63-87). Cham: Springer International Publishing.

[26] Gil, B.D., & Zeng, Y. (2022). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*, *29*(2), 460-475.

[27] Goni, O. (2022). Cybercrime and its classification. *Int. J. of Electronics Engineering and Applications*, *10*(1), 17.

[28] Grispos, G. (2021). Criminals: Cybercriminals. In *Encyclopedia of Security and Emergency Management* (pp. 84-89). Cham: Springer International Publishing.

[29] Jong, K. (2019). *Detecting the online romance scam: Recognising images used in fraudulent dating profiles* (Master's thesis, University of Twente).
[30] Khan, A. A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws*, *13*(4), 44.
[31] Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, *9*(2), 205.
[32] Mahmud, S. R. (2020). The effectiveness of Facebook advertisements on purchase intention of customers in Malaysia. *South Asian Journal of Social Sciences and Humanities*, *1*(1), 97-104.
[33] McCoy, D., Park, Y., Shi, E., & Jakobsson, M. (2016). Identifying scams and trends. *Understanding social engineering based scams*, 7-19.
[34] Muhammud, F. S., & Muhammad, H. (2022). Cybercrime through love scams: What women should know?. *Journal of Contemporary Islamic Studies*, *8*(2), 41-54.
[35] Paat, Y. F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18-40.
[36] Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health and mental health services research*, *42*, 533-544.
[37] Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology*, *14*(1), 81-105.
[38] Rahaman, M. M. (2022). Recent advancement of cyber security: Challenges and future trends in Bangladesh. *Saudi Journal of Engineering and Technology*, *7*(6), 278-289.
[39] Rahman, D. A. M., & Islam, S. (2022). *Financial and Social Costs Perspective Impacts of Cybercrime in the UAE: Policy-Guidance Addressing the Problem in Piecemeal Approach*. SSRN.
[40] Rege, A., & Bleiman, R. (2020, June). Ransomware attacks against critical infrastructure. In *Proc. 20th Eur. Conf. Cyber Warfare Security* (p. 324).
[41] Rehman, S., & Manickam, S. (2023). Towards a Cybersecurity Awareness Program for Non-Technical Audiences in Malaysia. In *Cybersecurity for Decision Makers* (pp. 85-97). CRC Press.
[42] Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, *17*(2), 164-196.
[43] Tomas, F., & Zanden, T. (2023). There Are Layers to Liars: A Systematic Literature Review of Online Dating Deception.
[44] Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.
[45] Yesmen, N., & Ahmed, N. (2022). The nature and challenges of cyber policing: A study on criminal investigation department (cid), dhaka, bangladesh. *Asian Journal of Sociological Research*, 210-214.