

## Original Article

# Economic Impact of Cyber Attacks: Lesson from a Real-World Fraudulent Investment App Causing Financial Losses

Naru Venkata Rajasekhara Reddy  
VVR Technos proprietor,

Manuscript ID:  
IJERSD-2026-020102

ISSN: 3067-2325

Volume 2

Issue 1

Pp. 5-8

February 2026

Submitted: 05 Jan. 2026

Revised: 15 Jan. 2026

Accepted: 10 Feb 2026

Published: 28 Feb 2026

### Correspondence Address:

Naru Venkata Rajasekhara Reddy  
VVR Technos proprietor,  
Email: [svurajasekhar@gmail.com](mailto:svurajasekhar@gmail.com)

Quick Response Code:



Web: <https://rlgjaar.com>

DOI: [10.5281/zenodo.18679573](https://doi.org/10.5281/zenodo.18679573)

DOI Link:  
<https://doi.org/10.5281/zenodo.18679573>



Attribution-NonCommercial-  
ShareAlike 4.0 International



## Abstract

*This paper investigates a real-world cyber fraud involving a fake investment mobile application that deceived users into depositing varying amounts of money with promises of high returns. The app operated by fraudulent entities used a fake investment platform to trick users into investing their money which the criminals then stole without delivering any actual returns. The financial loss suffered by victims in this incident amounts to approximately ₹5 lakhs. This study examines how fraudulent investment applications operate their economic effects and it presents essential prevention methods which include better user monitoring together with government regulations and cybersecurity systems that protect potential victims from similar scams.*

**Keywords:** Cybersecurity, Cyber Fraud, Investment Scam, Financial Loss, Mobile Applications, Cyber Attack, Fraud Prevention

## Introduction

The world financial system has experienced a major transformation because digital technologies developed at a fast pace which allows people to use mobile applications for banking and trading and investment services with greater simplicity than ever before. The investment platforms which operate through mobile devices became extremely popular because they provide users with easy access while requiring only basic skills and they offer fast financial returns. The growing need for digital financial systems brings both advantages and disadvantages because it results in an increase of cyber attacks through fraudulent investment applications. Cyber fraud involving fake investment mobile applications has emerged as a serious threat to individuals and financial ecosystems. Cybercriminals create applications which imitate real investment platforms to gain user trust while using fake advertisements and built profit dashboards and fake testimonials as their main tools. The applications attract users to deposit funds because they claim to deliver extremely high returns within a brief time frame. The fraudulent operators disappear after they have gathered enough money which leaves their victims facing substantial financial losses and few ways to recover their losses. India has experienced an increase of cyber fraud cases which target online investments during the past few years because cyber criminals now target all social classes. Cyber attacks produce two types of damage first they create direct financial losses and second they generate psychological distress which leads to financial problems and the loss of faith in digital financial systems. The economic impact of such fraud is particularly severe for small investors who often invest personal savings or emergency funds without adequate awareness of cybersecurity risks. Research studies about fraudulent investment applications now exist in academic literature because researchers examine how cybercrime functions at a regional level yet they study individual economic outcomes and operational fraud systems through case studies. Scammers run their operations through schemes which lead to financial damage so understanding their methods will help organizations build security systems to prevent their activities.

The current study examines an actual cyber fraud case which involved a fake investment mobile application that caused financial losses of around ₹5 lakhs. The study will investigate how the fraudulent app operates to establish its financial effects on users while assessing various protection methods which include user education and regulatory actions and cybersecurity systems. The paper intends to provide case-based evidence which will assist organizations to advance their digital financial security systems against current cybersecurity threats.

**Problem Statement:** The increasing popularity of mobile investment platforms has created more chances for cybercriminals to develop fake investment applications that deceive users. Many individuals, attracted by promises of high returns, invest their savings without verifying the authenticity of such platforms. The fraudulent applications lead to financial losses and cause psychological suffering while building distrust toward digital financial systems.

## Creative Commons

*This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution NonCommercial-ShareAlike 4.0 International](https://creativecommons.org/licenses/by-nc-sa/4.0/). The Creative Commons Attribution license allows re-distribution and re-use of a licensed work on the condition that the creator is appropriately credited*

## How to cite this article:

Reddy, N. V. R. (2026). Economic Impact of Cyber Attacks: Lesson from a Real-World Fraudulent Investment App Causing Financial Losses. *International Journal of Engineering Research for Sustainable Development*, 2(1), 5–8. <https://doi.org/10.5281/zenodo.18679573>

There is a research gap about real-world case studies which investigate how fake investment applications impact economics while demonstrating their operational systems since cyber fraud has become more common. The research investigates this issue through the examination of a real cyber fraud case which involved a fake investment mobile application.

**Scope of the Study:** The research will study a real-world cyber fraud case about a fake investment mobile application. The study investigates how mobile-based investment scams impact the economy while analyzing their attack methods and developing methods to stop such attacks. The research does not involve technical malware testing or extensive statistical analysis but it aims to provide practical knowledge to users and regulators and cybersecurity professionals.

#### Literature Review:

**Anderson et al. (2019)** conducted their research on cybercrime economic impacts worldwide and discovered that online financial fraud accounts for a major portion of total cybercrime damages. The study demonstrated that investment scams result in immediate monetary damages which subsequently create lasting economic damages for their victims. The research team discovered that economic cybercrime constitutes a serious threat because online investment fraud shows rapid expansion. The authors highlighted that weak regulation and cross-border anonymity increase fraud success rates. **Cross (2021)** Cross studied how investment fraud victims experience digital financial services through their reactions to financial losses and their emotional distress and trust destruction. The authors of the study examined how fraud affects people who have been victimized and they found that cyber-enabled investment scams cause excessive harm to small investors. The study required development of policies which would concentrate on helping victims. **Kshetri (2020)** Kshetri investigated emerging market cybercrime activities and discovered that mobile investment application fraudsters use digital illiteracy together with nonexistent regulatory systems. The research found that people who lack cybersecurity knowledge become more vulnerable to investment scams which promise high returns according to **Holtfreter et al. (2020)**. **Chang & Chen (2019)** Chang and Chen investigated how cybersecurity incidents impact consumer trust and their research found that financial cyber fraud causes major damage to trust in digital platforms. The authors studied cyber-enabled financial crimes but found that mobile investment scams increased because criminals could easily access the internet while remaining anonymous according to **Broadhurst et al. 2021**. The study examined deceptive design elements that fraudulent fintech platforms use to create fake profit dashboards which trick users into making more investments according to **Wang Lee and Wang 2020**. **Omarini** explained that digital banking cybersecurity risks matter because fraudulent investment applications create systemic financial security problems which need regulation according to **Omarini 2021**. **Gai Qiu and Sun 2020** The researchers studied security problems that fintech businesses face while showing how artificial intelligence technology helps identify fraudulent financial activities which include fake investment schemes. **Furnell and Shah 2022** The researchers studied cybersecurity awareness problems and discovered that investment-related cyber fraud succeeds because users lack proper education about security threats. The researchers studied cyber fraud trends in India and discovered that mobile investment scams have increased because of rapid fintech adoption and low public awareness according to **Gupta Agrawal and Yamaguchi 2021**. **Reddy & Reddy (2022)** This study analyzed digital payment fraud in India and reported that investment-related cyber fraud causes severe financial distress among middle- and lower-income users. **Albladi and Weir 2019** The researchers studied social engineering attacks and discovered that online investment scams use persuasion techniques which enable perpetrators to win their victims trust. The European Union Agency for Cybersecurity **ENISA 2023** reported that fraudulent financial applications now represent one of the fastest-growing cyber threats which require governments to improve their regulatory responses.

#### Objectives of the Study

1. To examine the operational mechanism of a fraudulent investment mobile application
2. To analyze the economic impact of the cyber fraud on affected users
3. To identify the cyber-attack techniques used in fake investment apps
4. To assess the risks posed by fraudulent mobile investment platforms
5. To suggest preventive strategies involving user awareness, regulatory measures, and cybersecurity technologies

#### Research Methodology

This study adopts a **descriptive case study research design** to examine the economic impact of a real-world cyber fraud incident involving a fraudulent investment mobile application. The methodology is designed to systematically analyze the operational mechanism of the scam, the nature of the cyber attack, and the financial consequences experienced by victims.

##### 1. Research Design

The research follows a descriptive and exploratory approach, focusing on an in-depth examination of a single real-world cyber fraud case. The case study method provides an effective research design which permits researchers to study detailed aspects of cybercrime cases and their actual economic effects.

##### 2. Nature and Sources of Data

The study is based on qualitative and secondary data, supplemented by limited primary inputs. Primary Data Informal interactions and verbal accounts from victims affected by the fraudulent investment app, focusing on the amount invested, method of deception, and financial consequences. Secondary Data Data were collected from Cybercrime complaint summaries News reports and verified media sources Government and regulatory reports on cyber fraud Published academic journals and cybersecurity studies.

##### 3. Sample Size and Sampling Technique

The sample consists of more than 20 victims who were affected by the fraudulent investment mobile application. The research used purposive sampling because its goal was to identify people who suffered financial losses through cyber fraud activities.

##### 4. Tools and Techniques of Data Collection

- Review of victim complaints and narratives
- Analysis of the fraudulent app's operational features, such as profit dashboards and referral schemes
- Examination of publicly available information related to the app's promotion and disappearance

##### 5. Method of Data Analysis

- The research team applied qualitative content analysis to examine the collected data. The analysis focused on:
- Identifying common patterns in fraud techniques
- Estimating total financial loss incurred by victims
- Understanding the economic and psychological impact of the cyber attack

- Categorizing preventive and mitigation measures

## **6. Ethical Considerations**

The study maintains strict ethical standards. The research team has protected victim identities by keeping their information secret and they have not revealed any financial details that belong to victims. The research relies only on voluntarily shared information and publicly available data sources.

### **Case Study: Fraudulent Investment App**

#### **1. Background of the Case**

The mobile-based investment application under examination operated as a fake financial system which promised investors substantial earnings within a brief time frame. The application reached its audience through aggressive marketing tactics which used social media platforms and messaging applications and online referral networks. The system presented itself as a safe investment option which would generate high returns to attract people who lacked advanced investment knowledge.

#### **2. Modus Operandi of the Fraudulent App**

The application intended for users to start making deposits after they finished their registration process. The application interface displayed fabricated profit figures and transaction histories which created a false financial growth display to users. The system offered referral incentives to users which made them invest larger amounts while bringing new users to the platform. The application blocked user access after it had gathered enough financial assets while users lost their ability to retrieve their invested funds. The app operators employed fake identities together with untraceable digital methods which created obstacles for recovery efforts.

#### **3. Economic Impact on Victims**

The case reported total financial losses that reached approximately ₹5 lakhs which impacted more than 20 victims. The victims lost both their personal savings and emergency funds. The bank accounts associated with the transactions experienced temporary freezes because of suspicious activity which created further financial difficulties. The economic impact extended beyond direct monetary loss, leading to disruption of daily financial activities.

### **Prevention and Mitigation Strategies**

#### **• User Awareness and Vigilance**

User awareness functions as an essential factor that stops investment-related cyber fraud. People must authenticate investment applications through authenticity verification and regulatory approval checks while they need to avoid platforms that guarantee or above-normal return rates. User education about common red flags enables them to protect themselves from becoming victims to digital threats which exist in their online environment.

#### **• Regulatory and Institutional Measures**

The regulatory authorities need to impose more strict regulations which require mobile investment applications to complete mandatory registration processes and undergo regular audits and develop capabilities for real-time system monitoring. The financial regulators need to work together with app stores and law enforcement agencies to develop systems which can quickly detect and eliminate fraudulent applications. 5.3 Technological Solutions Advanced cybersecurity technologies which include AI-driven fraud detection systems and secure authentication mechanisms and transaction monitoring tools enable organizations to detect suspicious activities during their initial development phase. App stores need to establish strict application review procedures which will stop fraudulent applications from obtaining approval for distribution.

### **Impact of Cyber Attacks: Beyond Financial Loss**

The initial result of cyber attacks shows financial losses as their most obvious effect. Cyber attacks create effects that go beyond their monetary destruction because they create effects that extend beyond their financial impact. Cyber fraud victims who experience fraudulent investment applications face extreme psychological and social and institutional effects which disrupt their entire existence. Cyber attacks create non-financial effects which demonstrate the complete human and societal impact after these attacks occur.

Psychological distress stands as one of the most dangerous effects which cyber fraud creates. Victims experience anxiety and depression together with shame and self-blame after they discover their deception. People experience emotional trauma because they lose their personal savings which includes both life savings and emergency funds. Digital financial services cause some victims to develop an ongoing fear which makes them unable to use these services and this fear restricts their financial access and their ability to use technology.

The digital financial system faces trust erosion because cyber attacks. Fraudulent investment platforms cause victims to lose their trust in all legitimate mobile applications and online banking and fintech services. Users who lose trust in digital financial technologies will stop using these technologies which creates a barrier to digital economic growth and financial digitization efforts. The main effect of this situation leads to interruptions in essential financial operations. During investigations, banks usually freeze or place liens on accounts that show suspicious activity. The restrictions stop victims from accessing their rightful money which they need to pay bills and cover their home expenses and their business needs. The economically vulnerable population faces severe financial harm because of these restrictions which create difficulty for them to access their funds. The social consequences of cyber fraud lead to victims experiencing stigma and embarrassment which creates difficulties in their relationships with both family and friends. Victims of financial crimes face social pressure to hide their losses which helps fraudsters to operate without any hindrance. Cyber attacks create extreme stress which can result in mental health emergencies thus showing the necessity of providing emotional support together with financial solutions.

### **Discussion**

The current research demonstrates how fraudulent investment mobile applications have become an increasing danger within the digital financial system. The case analysis demonstrates how cybercriminals exploit technological accessibility and human trust to execute investment-related cyber fraud. The results show that even minor cybersecurity breaches lead to severe financial damage which affects people who lose their savings because they lack knowledge about cybersecurity risks.

The study proves that cyber attacks produce effects which go beyond their financial costs because they damage mental health and decrease people's confidence in online banking systems. The discussion emphasizes that organizations need to adopt multi-layered prevention systems which require both user education and governmental control and modern cybersecurity solutions. The results demonstrate that digital financial services need to protect themselves against investment-related cyber fraud through collaboration among users and regulators and financial institutions and technology vendors.

## Conclusion

The present study examined a real-world cyber fraud incident involving a fraudulent investment mobile application and analyzed its economic impact on victims. The results show that cyber attacks lead to major financial losses which cause psychological problems and decrease trust in digital financial systems. Investment-related cyber fraud requires organizations to implement three fundamental elements which include user education and proper regulatory systems and advanced cybersecurity defenses. The protection of individuals and the secure development of digital financial systems depend on these operational areas which require enhancement. Future research may focus on large-scale empirical studies and advanced detection mechanisms to further enhance cybersecurity resilience.

## Acknowledgment

I would like to express my sincere gratitude to all the individuals who supported and contributed to the completion of this research on the economic impact of cyber-attacks, particularly the case study of a fraudulent investment mobile application. My heartfelt thanks go to the victims who courageously shared their experiences and financial details, enabling a deeper understanding of the operational mechanisms and economic consequences of the cyber fraud. Without their cooperation and trust, this case-based analysis would not have been possible.

I also extend my appreciation to cybersecurity professionals, legal advisors, and financial experts who provided valuable insights into the functioning of fraudulent digital platforms and the regulatory challenges involved in controlling such cyber threats.

Special thanks to academic researchers and authors whose published works in cybersecurity, fintech security, and cyber fraud prevention provided the theoretical foundation for this study. Their contributions significantly strengthened the analytical framework of this paper.

## Financial support and sponsorship

Nil.

## Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## References

1. Albladi, S. M., & Weir, G. R. S. (2019). Vulnerability to social engineering in cybersecurity. *Computers & Security*, 83, 101701. <https://doi.org/10.1016/j.cose.2019.101701>
2. Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the cost of cybercrime. *Journal of Cybersecurity*, 5(1), tyz003. <https://doi.org/10.1093/cybsec/tyz003>
3. Broadhurst, R., Chang, L. Y. C., Trinh, T., & Bouhours, B. (2021). Cybercrime and cyber-enabled crime. *Computers & Security*, 103, 102232. <https://doi.org/10.1016/j.cose.2021.102232>
4. Button, M., Lewis, C., & Tapley, J. (2021). Not a victimless crime. *Computers & Security*, 105, 102211. <https://doi.org/10.1016/j.cose.2021.102211>
5. Chang, S. E., & Chen, Y. (2019). When IT systems fail. *Information & Management*, 56(6), 103146. <https://doi.org/10.1016/j.im.2019.03.004>
6. Cross, C. (2021). Victims of investment fraud. *Deviant Behavior*, 42(5), 595–610. <https://doi.org/10.1080/01639625.2021.1883014>
7. Furnell, S., & Shah, J. N. (2022). Cybercrime and cybersecurity awareness. *Computers & Security*, 114, 102573. <https://doi.org/10.1016/j.cose.2022.102573>
8. Gai, K., Qiu, M., & Sun, X. (2020). A survey on fintech security. *Journal of Network and Computer Applications*, 165, 102805. <https://doi.org/10.1016/j.jnca.2020.102805>
9. Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2021). Cyber fraud detection in fintech systems. *International Journal of Information Security*, 20(5), 547–563. <https://doi.org/10.1007/s10207-021-00512-4>
10. Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2020). Low self-control and fraud victimization. *Computers in Human Behavior*, 103, 106467. <https://doi.org/10.1016/j.chb.2020.106467>
11. Kshetri, N. (2020). Cybercrime and cybersecurity in emerging economies. *Telecommunications Policy*, 44(10), 101353. <https://doi.org/10.1016/j.tele.2020.101353>
12. Levi, M., Smith, R. G., & Hutchings, A. (2020). The impact of economic cybercrime. *British Journal of Criminology*, 60(2), 1–20. <https://doi.org/10.1093/bjc/azaa012>
13. Omarini, A. (2021). Fintech and cybersecurity challenges. *Electronic Markets*, 31(3), 587–596. <https://doi.org/10.1007/s12525-021-00466-3>
14. Reddy, K. S., & Reddy, V. R. (2022). Digital payment fraud in India. *Journal of Indian Business Research*, 14(3), 389–404. <https://doi.org/10.1108/JICES-10-2021-0094>
15. Wang, Y., Lee, M., & Wang, H. (2020). Trust in fintech platforms. *Decision Support Systems*, 137, 113366. <https://doi.org/10.1016/j.dss.2020.113366>
16. ENISA. (2023). *Cybersecurity threat landscape*. European Union Agency for Cybersecurity. <https://doi.org/10.2824/063410>