VISVESVARAYA TECHNOLOGICAL UNIVERSITY

JNANASANGAMA, BELAGAVI - 590018

Cryptography and Cyber security (21CSE163)

Report
on
Aadhaar Biometric Fraud

Submitted in partial fulfillment for the award of the degree of

Bachelor of Engineering

in

COMPUTER SCIENCE & ENGINEERING

Submitted by

Skanda J (1BG21CS127)

Submitted to

Dr. Rajashree Soman
Associate Professor, Dept. of CSE
BNMIT, Bengaluru

B.N.M. Institute of Technology

An Autonomous Institution under VTU

Approved by AICTE, Accredited as a grade A Institution by NAAC. All eligible branches – CSE, ECE, EEE, ISE & Mech. Engg. are Accredited by NBA for academic years 2021-22 to 2024-25.

URL: www.bnmit.org

Department of Computer Science and Engineering

2023 - 24

TABLE OF CONTENTS

Contents	Page No.
1 – Introduction	1
2 – Details of Cybercrime	1
3 – Impact Assessment	3
4 – Government Response	4
5 – Solution	5
6 – Conclusion	7
7 – References	8

ABSTRACT

This report delves into a recent cybercrime case in Bihar, India, where criminals exploited weaknesses in the Aadhaar Enabled Payment System (AePS) to steal money from bank accounts without requiring OTPs or phone calls. The perpetrators accessed Aadhaar biometric data from publicly available government land records and fabricated fake fingerprints to bypass security measures, enabling unauthorized withdrawals. This incident underscores critical security gaps in the AePS and the risks associated with biometric data misuse.

The report evaluates the financial, psychological, and systemic repercussions of the crime and details the government's response. It also offers solutions, such as strengthening cybersecurity protocols, increasing public awareness, and implementing technological advancements to prevent future incidents. This case highlights the necessity for robust data protection strategies, continuous digital infrastructure monitoring, and cooperative efforts among government bodies, financial institutions, and the public to protect sensitive personal information in a growing digital financial landscape.

Introduction

In a recent cybercrime incident in Bihar, a gang managed to steal money from bank accounts without requiring an OTP or making a phone call. The perpetrators exploited Aadhaar biometric data, which they obtained from government websites containing land records. This method of theft underscores significant vulnerabilities in the security of personal data and the potential for misuse of biometric information. This report delves into the details of the incident, the methods employed by the criminals, and the broader implications for data security and privacy.

Details of Cybercrime

The cybercrime in Bihar involved a gang that exploited vulnerabilities in the Aadhaar Enabled Payment System (AePS) to steal money from bank accounts without needing an OTP or a phone call [1]. The AePS allows for transactions such as withdrawals and deposits using only the Aadhaar number and biometric authentication, typically a fingerprint. This system, intended to promote financial inclusion in rural areas, became a target for cybercriminals due to its reliance on easily accessible biometric data.

Data Collection

- Publicly Available Biometric Data: The gang accessed Aadhaar biometric information from government websites with publicly accessible land records. These records often include fingerprints used for land transaction verification.
- Fake Fingerprint Cloning: Using silicone-based latex glue and other techniques, the fraudsters created fake fingerprints, which they used to deceive biometric scanners.

Exploiting AePS

- Biometric Authentication: Using the cloned fingerprints, the gang members authenticated themselves at AePS points, such as micro-ATMs and authorized business correspondents, to facilitate transactions.
- Withdrawals Without OTP: The system allowed them to withdraw money from victims' bank accounts using only the Aadhaar number and cloned fingerprints, bypassing the need for an OTP or any other form of additional verification.

Technical Vulnerabilities

- Lack of Live Finger Detection: Some private biometric scanners used by AePS operators could not detect if a fingerprint was from a live finger, making them vulnerable to fake fingerprints.
- Default Activation of AePS: Many individuals unknowingly activated AePS when linking their Aadhaar to their bank accounts. Unlike other banking services, AePS was often activated by default without explicit consent, increasing the risk of unauthorized access.

Countermeasures and Recommendations

- Locking Aadhaar Biometrics: Users are advised to lock their Aadhaar biometric information and unlock it only when necessary to prevent unauthorized access.
- Enhanced Security Measures: Improved security protocols for biometric scanners, such as incorporating live detection features, are essential to mitigate such fraud.
- Awareness Campaigns: Increasing awareness about the risks of linking Aadhaar to various services and educating users on safeguarding their biometric data is crucial.

Impact Assessment

The recent cybercrime incident in Bihar has far-reaching implications for both individuals and the broader system. This analysis explores the various impacts of the crime, from financial losses to the erosion of trust in digital and biometric systems, aiming to provide a comprehensive understanding of how such fraud affects different stakeholders and to highlight the importance of robust security measures.

Financial Impact

The primary impact of this cybercrime was financial, with victims suffering direct monetary losses due to unauthorized withdrawals from their bank accounts. Many affected individuals were from rural or semi-urban areas, where awareness about cyber threats is relatively low. The financial strain on these victims is exacerbated by their limited means to recover the stolen funds. Reports indicate that the stolen amounts ranged from a few hundred to several thousand rupees per victim, leading to substantial aggregate losses.

Psychological and Social Impact

The psychological effects of such fraud can be profound. Victims experience stress, anxiety, and a sense of violation upon realizing their hard-earned money has been stolen. This can lead to a loss of trust in digital financial systems and government-backed initiatives like Aadhaar. The social impact is also significant, as communities begin to distrust digital banking services, potentially reverting to cash-based transactions, which are less secure and more cumbersome.

Regulatory and Policy Impact

The cybercrime has prompted calls for stronger regulatory oversight and the implementation of more stringent security measures. Policymakers are urged to reconsider the default activation of AePS and to mandate explicit consent for its usage. Additionally, there is a need for enhanced public awareness campaigns to educate citizens about securing their biometric data and the potential risks associated with digital transactions.

Technological Impact

From a technological perspective, the incident underscores the necessity for advancements in biometric security. The current generation of biometric scanners needs to incorporate features like live detection to prevent the use of cloned fingerprints. This incident also calls for a reevaluation of how biometric data is stored and accessed, advocating for more secure and encrypted storage solutions.

Government Response

Upon discovering the cybercrime operation in Bihar, the government and law enforcement agencies took swift and significant actions [3]. The Bihar Police immediately initiated an investigation, which led to the arrest of eight individuals involved in the scam. The police detailed how the criminals exploited Aadhaar biometric data obtained from government land records to execute fraudulent transactions using the Aadhaar Enabled Payment System (AePS), bypassing the need for OTPs or phone calls.

The government responded by enhancing cybersecurity measures and reviewing the accessibility of sensitive data on public websites. Authorities emphasized the need for stricter data protection protocols and better awareness among citizens about safeguarding their personal information. Additionally, a Special Investigation Team (SIT) was formed to delve deeper into the case, aiming to uncover and prevent further misuse of Aadhaar data.

Furthermore, police departments across various states issued advisories to the public, urging them not to share Aadhaar details or fingerprints and to be cautious about phishing attempts. The response also included coordination with banking institutions to ensure better security for AePS transactions and increased monitoring of suspicious activities.

Solution

The resolution of the cybercrime case in Bihar involved a multi-faceted approach focusing on immediate actions, long-term strategies, and technological enhancements [4][5][6]. Following the identification and arrest of the key perpetrators, the authorities embarked on a thorough investigation to dismantle the entire operation and prevent future occurrences of similar frauds.

.

1. **Immediate Arrests and Investigation**:
    - The Bihar Police, aided by the cybercrime unit, promptly arrested eight individuals who were found to be directly involved in the cybercrime.
    - These arrests were pivotal in halting the ongoing fraudulent activities and gathering critical information on the modus operandi of the criminals.
    - The investigation revealed that the gang had exploited vulnerabilities in the Aadhaar Enabled Payment System (AePS) by using Aadhaar biometric data obtained from land records.
2. **Strengthening Cybersecurity Measures**:
    - In response to the incident, the government intensified cybersecurity measures.
    - This included conducting a security audit of public websites containing sensitive data to identify and rectify vulnerabilities.
    - The authorities also implemented stricter access controls and encryption protocols to safeguard Aadhaar data and other personal information from unauthorized access.
3. **Public Awareness and Education**:
    - Recognizing the importance of public awareness in preventing cybercrimes, the government launched awareness campaigns to educate citizens about the risks of sharing their Aadhaar details and biometric information.
    - These campaigns emphasized the importance of personal data security and provided guidelines on how to protect oneself from phishing and other fraudulent activities.

4. **Banking Sector Coordination**:
    - The government coordinated with banking institutions to bolster the security of AePS transactions.
    - This included enhancing authentication mechanisms and implementing additional layers of verification for high-risk transactions.
    - Banks were also instructed to monitor and report suspicious activities promptly to prevent unauthorized transactions.
5. **Technological Enhancements**:
    - To further secure the AePS and other digital payment systems, technological enhancements were introduced.
    - These included the integration of advanced biometric authentication technologies and artificial intelligence-driven monitoring systems to detect and flag suspicious activities in real time.
6. **Long-term Strategies**:
    - The government established a Special Investigation Team (SIT) to continue probing the incident and to develop long-term strategies for preventing such crimes in the future.
    - The SIT's mandate included reviewing current data protection laws and recommending improvements to ensure protection of citizens' personal data.

In conclusion, the comprehensive approach involving immediate arrests, strengthened cybersecurity measures, public awareness, banking sector coordination, technological enhancements, and long-term strategies successfully addressed the cybercrime incident in Bihar. These measures not only resolved the specific case but also fortified the overall cybersecurity infrastructure to prevent future occurrences of similar frauds.

Conclusion

The cybercrime incident in Bihar, where a gang exploited Aadhaar biometrics data to siphon money from bank accounts without the need for OTPs or phone calls, underscores significant vulnerabilities in digital payment systems and data security protocols. The swift and comprehensive response by the authorities, including the arrests of the perpetrators, the enhancement of cybersecurity measures, public awareness campaigns, and technological upgrades, has been crucial in addressing the immediate threat and preventing future occurrences of similar frauds. This case highlights the necessity for robust data protection mechanisms, continuous monitoring of digital infrastructures, and collaborative efforts between government entities, financial institutions, and the public to safeguard sensitive personal information. The lessons learned from this incident will inform future strategies to fortify digital security and protect citizens from evolving cyber threats.

References

[1] https://www.opindia.com/2024/07/bihar-gang-stole-money-from-bank-account-without-otp-or-phone-call-using-aadhar/

[2] https://www.boomlive.in/decode/cloned-fingerprints-scam-the-story-of-aadhaar-enabled-payment-system-22944