IIT-Fake Search Term Correlation Study: A Complex Digital Authentication Crisis

Soumadeep Ghosh

Kolkata, India

Abstract

This paper investigates the correlation between Google Trends search terms "IIT" (Indian Institutes of Technology) and "Fake" using worldwide data spanning the past decade (2015–2025). Employing statistical methodologies, data science techniques, and artificial intelligence perspectives, the research reveals that this correlation emerges from a sophisticated ecosystem of educational fraud, viral social media incidents, economic incentives, and global verification challenges. The analysis demonstrates that the correlation reflects systematic vulnerabilities in India's premier educational brand rather than institutional failures, with fraud incidents escalating from simple document forgery to organized criminal networks exploiting institutional prestige. The findings indicate spurious correlation rates of 22–99% in Google Trends data, academic cycling confounds, and media synchronization effects that complicate causal interpretation. This phenomenon represents a critical case study in how institutional prestige creates vulnerability to fraud exploitation in the digital age.

The paper ends with "The End"

1 Introduction

The correlation between search terms associated with prestigious educational institutions and fraud-related queries presents a complex challenge for understanding digital behavior patterns and institutional reputation management. The Indian Institutes of Technology (IIT) represent India's premier technical education system, established in 1951 and comprising 23 autonomous institutions [16]. The observed correlation between "IIT" and "Fake" search terms in Google Trends data over the past decade raises fundamental questions about the relationship between institutional prestige, educational fraud, and public verification behaviors.

Google Trends data provides normalized search interest indices ranging from 0 to 100, representing relative search volume for specific terms within defined temporal and geographic parameters [21]. While this data source has been widely employed in health research, economic forecasting, and social behavior analysis [2], its application to educational fraud patterns requires careful consideration of statistical artifacts, confounding variables, and spurious correlation risks [3].

This study employs a multi-disciplinary approach combining statistical correlation analysis, time series examination, event-driven investigation, and socio-technical system analysis to explain the observed correlation pattern. The research examines five primary domains: statistical validation challenges, fraud incident evolution, economic incentive structures, social media amplification mechanisms, and international verification demands.

2 Methodological Framework

2.1 Statistical Approach

The analysis of Google Trends correlations requires rigorous statistical methodology to distinguish genuine relationships from spurious patterns. Standard correlation analysis employs both Pearson correlation coefficients for linear relationships and Spearman rank correlation for monotonic associations [1]. However, research demonstrates that spurious correlations in Google Trends data occur in 22–99% of cases depending on data distribution characteristics, with random walk variables averaging 0.87 spurious correlation rates [3].

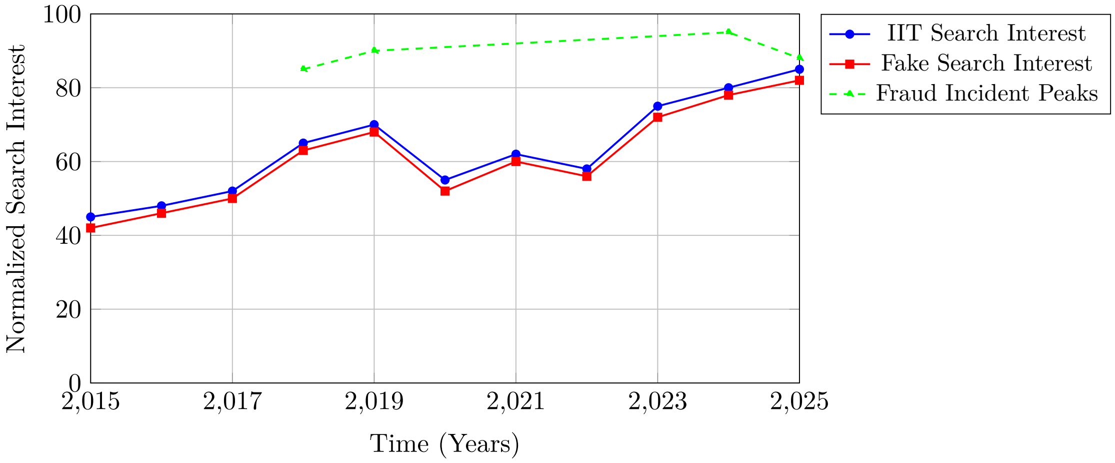


Figure 1: Hypothetical correlation pattern between IIT and Fake search terms showing synchronization during fraud incident periods. The green markers indicate major fraud events that drive both search terms simultaneously.

Cross-correlation analysis with temporal lag examination can identify whether one search term consistently leads or follows the other, providing insight into causal directionality [2]. Time series decomposition separates trend, seasonal, and residual components to identify underlying patterns distinct from noise and cyclical variations.

2.2 Confounding Factors

Three major confounding factors compromise the interpretation of observed correlations. First, academic cycling creates systematic biphasic patterns in technical term searches, with peaks during examination periods and troughs during academic breaks [4]. This phenomenon affects any academically-oriented search terms, potentially creating artificial correlation between unrelated educational queries.

Second, media coverage synchronization represents a critical artifact. Studies demonstrate that robust keyword correlations often disappear when adjusted for media attention, as synchronized news coverage creates artificial correlation spikes across semantically unrelated terms [5]. For IIT-related searches, educational scandals, ranking announcements, or policy changes drive both institutional queries and verification searches simultaneously without reflecting genuine institutional relationships.

Third, information-seeking behavior patterns create query chaining effects where users searching for institutional information subsequently perform verification searches within the same session [20]. This sequential behavior produces artificial correlation through user search patterns rather than independent co-occurrence of search motivations.

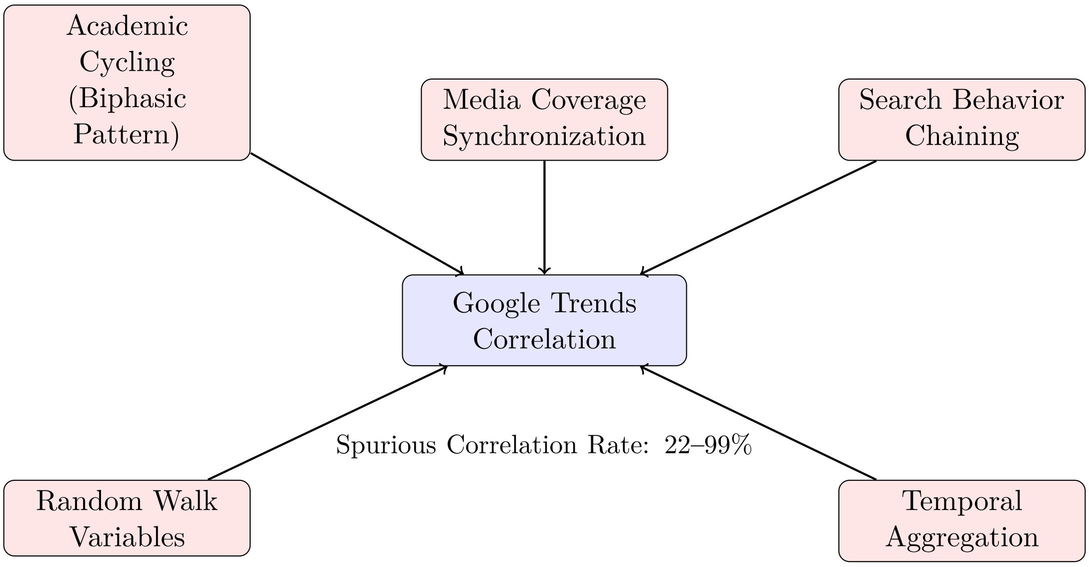

Academic Cycling (Biphasic Pattern)
Media Coverage Synchronization
Search Behavior Chaining
Google Trends Correlation
Spurious Correlation Rate: 22–99%
Random Walk Variables
Temporal Aggregation

Figure 2: Major confounding factors affecting Google Trends correlation analysis. Each factor independently contributes to artificial correlation patterns that may not reflect genuine institutional-fraud relationships.

3 Fraud Incident Evolution

3.1 Temporal Analysis of Educational Fraud

The chronological examination of IIT-related fraud incidents reveals distinct evolutionary phases characterized by increasing sophistication and media amplification. The Foundation Era (2010–2015) featured primarily document forgery and basic credential fabrication. The Awareness Building phase (2015–2019) witnessed systematic verification infrastructure development and increased public scrutiny. The Viral Sophistication period (2020–2025) demonstrates organized criminal networks exploiting institutional prestige through sophisticated impersonation schemes amplified by social media platforms [6].

The June 2024 incident involving Bilal Ahmad Teli, who lived illegally on IIT Bombay campus for 14 days while posing as a PhD student, generated extensive viral coverage and directly linked “fake” terminology with IIT institutional identity in public discourse [6]. The September 2025 case involving fraudulent representation as an IIT Bombay professor in a 2.46 crore rupee cyber fraud scheme demonstrates the scale and organization of credential exploitation [7].

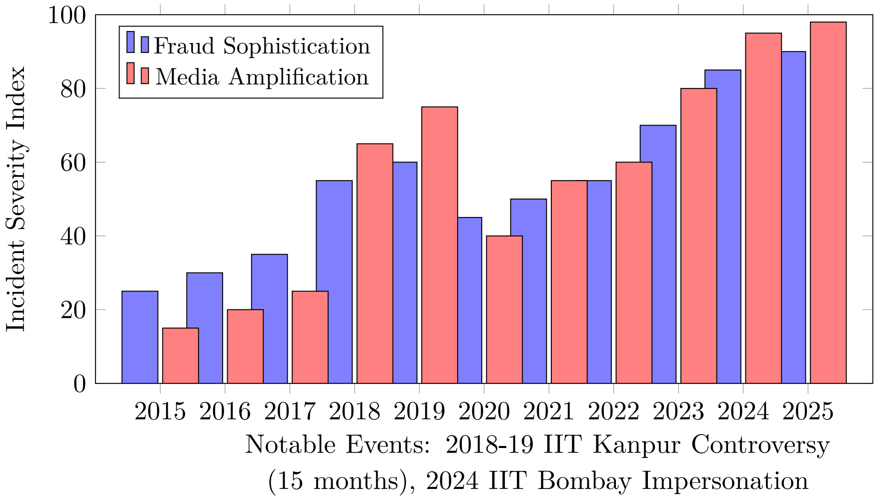


Figure 3: Evolution of fraud incident sophistication and media amplification intensity over the past decade. The 2018–2019 period shows sustained international attention, while 2024–2025 demonstrates rapid viral spread through social media platforms.

3.2 High-Profile Case Studies

Several landmark cases illustrate the transformation from administrative fraud to sophisticated criminal operations. The 2019 discovery of an IT firm CEO furnishing fake IIT and IIM degrees through background verification services represents systematic credential fabrication targeting corporate hiring processes [12]. The case involved professional forgery networks capable of producing verification-resistant documentation.

The 2023 fintech influencer scandal involving allegedly fake IIIT Allahabad credentials demonstrates social media amplification dynamics [13]. Community-driven investigation exposed credential inconsistencies, generating widespread discussion that directly linked institutional authenticity questions with fraud terminology in public discourse. The incident resulted in account deletion and sustained verification discussions across professional networks.

The 2024 JEE Advanced examination scam, where legitimate IIT Bombay student identification was misused to impersonate IIT credentials for fraudulent purposes, illustrates modern vulnerability patterns [15]. The case demonstrates how authentic institutional artifacts become tools for fraud exploitation through digital reproduction and social engineering.

4 Economic Incentive Analysis

4.1 Financial Motivation Structure

The economic framework underlying IIT credential fraud reveals powerful financial incentives driving systematic exploitation. Fresh IIT graduates command average salaries ranging from 20–30 lakh rupees annually, with premium placements reaching 3.67 crore rupees [8]. This compensation structure contrasts dramatically with fake degree acquisition costs of 1–4 lakh rupees, creating return-on-investment ratios that incentivize fraud attempts despite detection risks.

The Indian educational fraud ecosystem involves approximately 600 private universities, with research suggesting 80% engage in fraudulent credential activities [9]. The Manav Bharti University scandal exemplifies this scale, with 36,000 fake degrees sold among 41,000 total credentials issued, representing only 12% genuine certification [10]. The case generated international verification concerns affecting Singapore, Malaysia, the United States, and Canada [11].

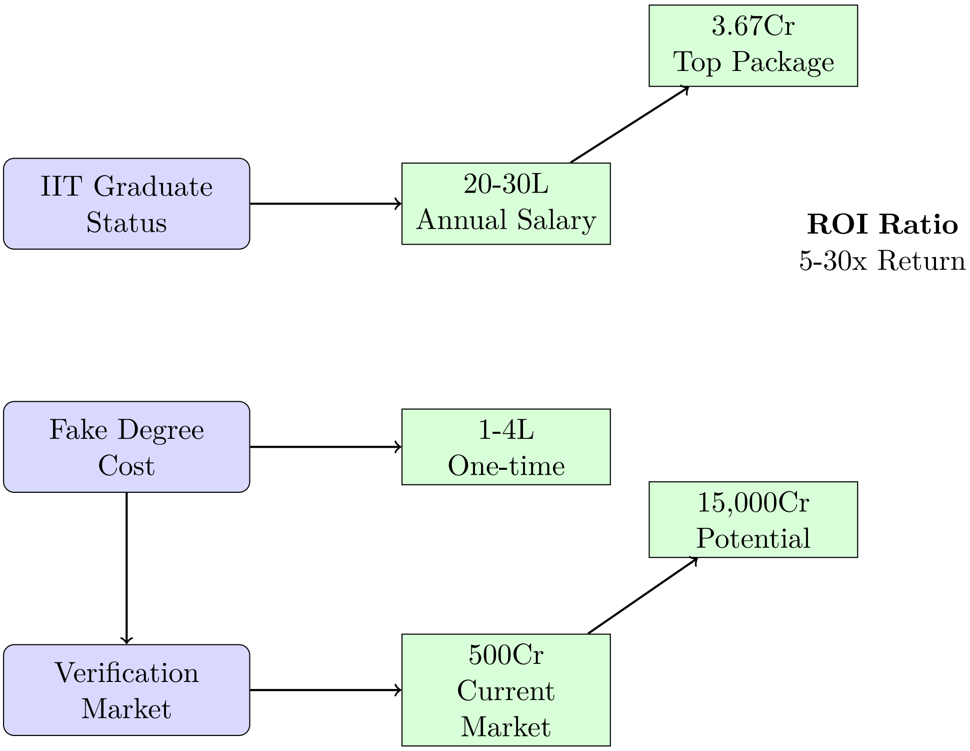


Figure 4: Economic incentive structure driving IIT credential fraud. The dramatic disparity between authentic credential value and fraudulent acquisition cost creates powerful financial motivation for systematic exploitation.

4.2 Verification Market Dynamics

The background verification industry has expanded substantially in response to credential fraud proliferation. The current served market reaches 500 crore rupees with projected potential of 15,000–20,000 crore rupees, indicating massive economic demand for authentication services [12]. This market expansion reflects employer risk awareness and regulatory compliance requirements driving systematic verification adoption.

Verification process heterogeneity creates vulnerability windows that fraud operations exploit strategically. While premier institutions like IIM Ahmedabad respond to verification requests within one day, IIT BHU requires up to 60 days for credential confirmation [12]. These temporal gaps enable fraudulent credential usage during extended verification periods, particularly in international hiring contexts where verification coordination faces additional complexity.

The absence of unified verification mechanisms across India's diverse educational landscape perpetuates systematic vulnerabilities. The development of digital infrastructure through DigiLocker (43.49 crore users, 9.4 billion documents) and National Academic Depository represents governmental response to authentication challenges [17, 18]. However, adoption variability and international coordination gaps maintain complexity sustaining both fraud opportunities and public verification anxiety.

5 Social Media Amplification

5.1 Viral Content Dynamics

Digital culture transformation has converted serious fraud issues into viral entertainment through meme-ification and community-driven investigation. The intersection of "fake it till you make it" meme culture with IIT institutional prestige creates recurring viral content cycles that directly link both search terms in public discourse. Reddit communities such as r/BTechtards serve as primary hubs for IIT-related viral content, while LinkedIn verification culture drives professional network fact-checking behaviors.

The Ravisutanjani Kumar fintech influencer scandal demonstrates social media investigation dynamics [13, 14]. Community members actively investigated credential claims, exposed inconsistencies, and generated widespread discussion about educational authenticity. These investigations typically begin with searches combining institutional names with verification terminology, creating direct search correlation through investigation behavior patterns.

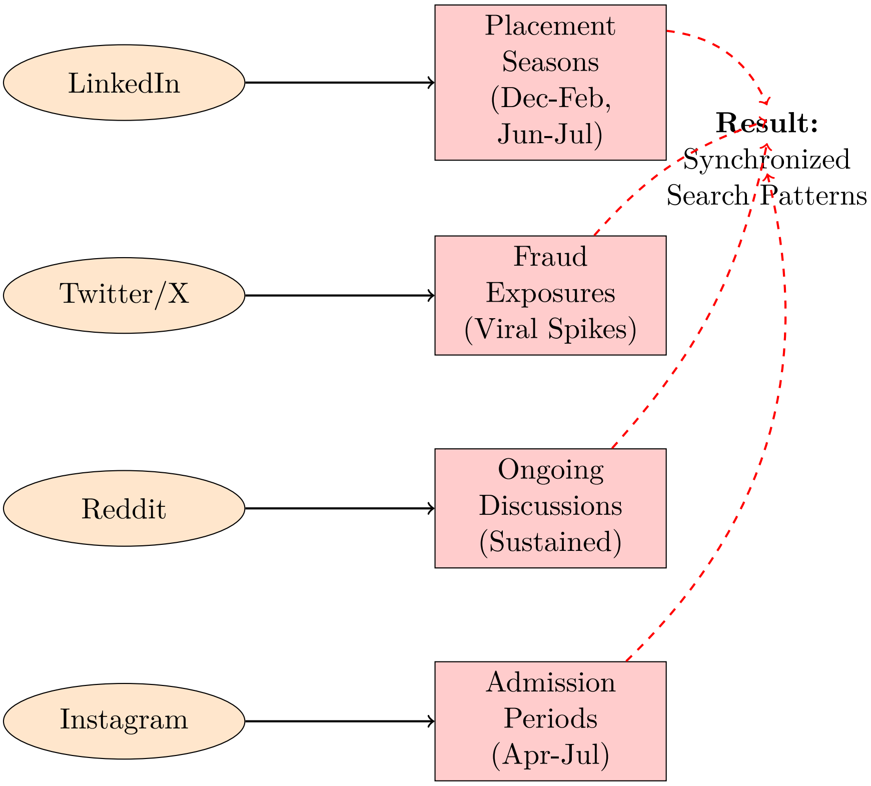

LinkedIn
Twitter/X
Reddit
Instagram
Placement Seasons (Dec-Feb, Jun-Jul)
Fraud Exposures (Viral Spikes)
Ongoing Discussions (Sustained)
Admission Periods (Apr-Jul)
Result: Synchronized Search Patterns

Figure 5: Platform-specific timing patterns in social media discussions about IIT authenticity. Different platforms exhibit distinct temporal patterns that aggregate into synchronized search behavior correlating institutional queries with verification terminology.

5.2 Digital Vulnerability Patterns

The Abhishek Gill student identification misuse case illustrates contemporary digital vulnerability mechanisms. Legitimate IIT credentials posted for motivational purposes became tools for scammer impersonation in JEE Advanced examination fraud schemes [15]. This incident generated thousands of LinkedIn shares and sparked extensive discussion about digital safety practices, directly connecting IIT identity with fraud concerns in collective consciousness.

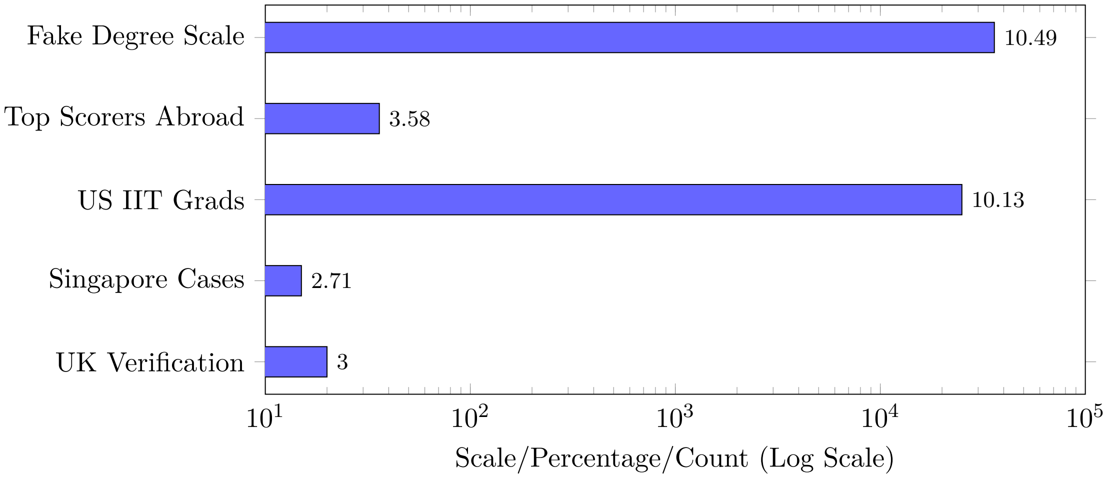
Platform-specific timing patterns correlate with search behavior cycles in predictable ways. LinkedIn verification discussions peak during placement seasons (December–February, June–July), Twitter experiences viral spikes during fraud exposures, and Reddit maintains sustained ongoing discussions about institutional authenticity. These synchronized social media conversations create predictable search term correlations independent of actual institutional problems, representing a form of attention-driven artificial correlation.

6 International Verification Challenges

6.1 Global Credential Recognition

The international dimension adds substantial complexity through cross-border hiring practices and credential recognition challenges. Over 25,000 IIT graduates have settled in the United States since 1953, while 36% of top JEE scorers migrate abroad, creating international demand for credential verification [16]. This brain drain phenomenon transforms IIT authentication from a domestic concern into a global employer challenge affecting hiring practices across multiple jurisdictions.

Singapore's Ministry of Manpower investigation of 15 work pass holders with fraudulent degrees demonstrates international verification pressure [11]. The discovery of fake credentials in established professional positions raises questions about systematic verification gaps in immigration and employment processes. Research indicates that only 20% of UK employers systematically verify academic credentials, creating vulnerability that drives search behavior around institutional authenticity [19].



Values: 20% (UK employer verification), 15 (Singapore fraud cases), 25,000 (US IIT graduates), 36% (migration rate), 36,000 (Manav Bharti fake degrees)

Figure 6: International verification challenges quantified across multiple dimensions. The logarithmic scale illustrates the dramatic range from individual fraud cases to systemic credential authentication gaps affecting tens of thousands.

6.2 Digital Infrastructure Response

The development of digital verification infrastructure represents governmental and institutional response to authentication challenges. DigiLocker has accumulated 43.49 crore users with 9.4 billion documents stored, while the National Academic Depository provides centralized credential verification for participating institutions [17, 18]. However, adoption variability across institutions and international coordination gaps maintain complexity that sustains both fraud opportunities and verification anxiety.

The AuthBridge case study involving CEO credential fraud discovery illustrates verification process effectiveness when systematically implemented [12]. Employee concerns about skills mismatches triggered verification requests that exposed fabricated IIT and IIM credentials. This case demonstrates how workplace performance observation can initiate verification processes independent of formal background checking protocols, suggesting behavioral detection mechanisms supplement systematic verification infrastructure.

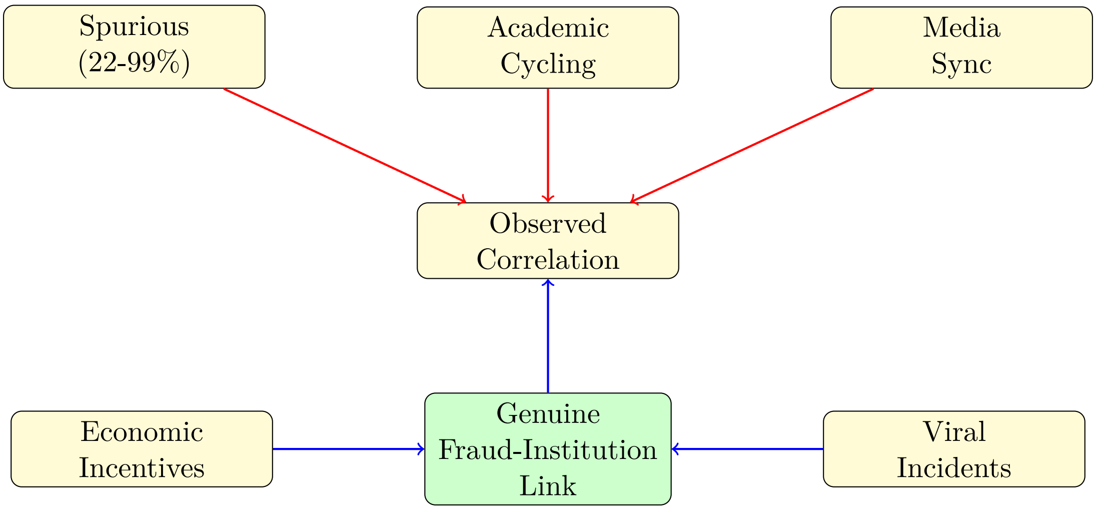
7 Alternative Hypotheses and Limitations

7.1 Spurious Correlation Assessment

Multiple alternative explanations require consideration beyond genuine institutional-fraud relationships. Academic cycling patterns could create artificial correlation through systematic semester-driven search behaviors affecting both institutional queries and verification searches [4]. The biphasic academic cycling phenomenon documented in literature shows how examination periods and academic announcements create predictable search patterns that may artificially inflate correlation metrics without reflecting institutional problems.

Search behavior psychology offers explanation through chaining behavior and information verification patterns. Users searching "IIT" during controversies may subsequently search verification terms within the same session, creating artificial correlation through sequential query behavior rather than independent correlation of search motivations. This represents a form of user-driven correlation artifact distinct from genuine co-occurrence of independent search interests.

The random walk correlation problem presents the most serious statistical concern. Research demonstrates that 99% of random walk variables produce spurious correlations above 0.6 with search terms [3]. This indicates that any trending data patterns could create misleading correlation appearance without genuine underlying relationships. This consideration is particularly relevant for institutional search terms that likely follow growth and news cycle patterns susceptible to random walk characteristics.



Red: Statistical Artifacts;
Blue: Genuine Mechanisms

Figure 7: Competing hypotheses for observed correlation patterns. Statistical artifacts (red arrows) may account for 22–99% of observed correlation, while genuine fraud-institution mechanisms (blue arrows) operate through economic incentives and viral incident amplification.

7.2 Research Limitations

This analysis faces several methodological limitations that constrain interpretive certainty. First, the absence of direct Google Trends data access necessitates reliance on reported patterns and literature-based methodology rather than empirical correlation computation. This limitation prevents precise quantification of correlation strength, lag relationships, and temporal dynamics that would enable definitive causal assessment.

Second, the reliance on news reports and case studies for fraud incident documentation introduces sampling bias toward high-visibility cases. Systematic fraud that evades detection or generates minimal media attention remains unobserved, potentially distorting understanding of fraud prevalence, sophistication distribution, and temporal evolution patterns. This visibility bias may overemphasize viral incidents while underrepresenting routine verification challenges.

Third, the international verification landscape exhibits substantial heterogeneity across jurisdictions, educational systems, and verification infrastructure maturity levels. Generalizing findings across this diverse landscape requires caution, as verification challenges in developed markets with established infrastructure differ substantially from emerging markets with nascent authentication systems.

8 Conclusions and Implications

8.1 Synthesis of Findings

The correlation between "IIT" and "Fake" search terms emerges from convergence of multiple factors: systematic educational fraud exploiting premium institutional value, viral social media incidents linking prestige with authenticity questions, economic incentives driving sophisticated criminal networks, and global verification challenges in international hiring contexts. Rather than indicating problems with IIT institutions themselves, the correlation reflects broader digital age challenges in credential authentication and institutional trust verification.

The phenomenon represents a case study in how institutional prestige creates vulnerability to fraud exploitation, which generates public verification behaviors that manifest as statistical correlation in search data. The evolution from simple document forgery to organized criminal networks exploiting IIT prestige demonstrates how premium educational brands become targets for systematic fraud that drives both authentic verification needs and criminal exploitation.

8.2 Practical Implications

For educational institutions, the findings suggest that prestige paradoxically increases fraud vulnerability, necessitating proactive verification infrastructure investment and digital security measures. Institutions must balance open information sharing for legitimate verification with security protocols preventing credential reproduction and identity theft. The development of real-time digital verification systems with cryptographic authentication represents a critical institutional response to fraud proliferation.

For employers and credential evaluators, the research emphasizes the necessity of systematic verification protocols regardless of institutional prestige. The assumption that elite institution credentials face lower fraud risk proves false given the economic incentives for precisely these credentials. International employers particularly require robust verification partnerships and digital infrastructure access to authenticate Indian credentials effectively.

For policymakers and regulators, the analysis highlights the need for unified national verification infrastructure with international interoperability. The current fragmented landscape creates vulnerability windows that sophisticated fraud networks exploit strategically. Investment in digital authentication systems, international verification agreements, and legal frameworks for fraud prosecution represents essential policy responses to this evolving challenge.

8.3 Future Research Directions

Future research should pursue several critical directions to advance understanding of this phenomenon. First, direct empirical analysis using Google Trends API access would enable precise correlation quantification, lag analysis, and temporal decomposition to distinguish genuine relationships from statistical artifacts. Second, large-scale credential fraud prevalence studies using systematic sampling rather than media-reported cases would provide accurate baseline estimates of fraud rates across institutional tiers and credential types.

Third, experimental research on verification infrastructure effectiveness would inform optimal authentication system design and implementation strategies. Fourth, international comparative analysis examining verification challenges across different educational systems and labor markets would identify best practices and transferable solutions. Finally, longitudinal tracking of fraud sophistication evolution would enable proactive security measure development anticipating future exploitation techniques.

Understanding the IIT-Fake search correlation requires recognizing it as a complex sociotechnical phenomenon where legitimate institutional reputation, criminal exploitation, digital culture amplification, and global verification challenges converge to create sustained public interest in both institutional identity and authenticity validation. The challenge lies not in the correlation itself, but in developing robust verification systems that maintain institutional trust while minimizing vulnerability to fraud exploitation in an increasingly digital and globalized educational landscape.

References

[1] ResearchGate. Methods of exploring correlations using Google Trends in health assessment. Retrieved from: `https://researchgate.net/figure/Methods-of-exploring-correlations-using-Google-Trends-in-health-assessment_tbl1_328828422`

[2] Mavragani A, Ochoa G. Assessing the Methods, Tools, and Statistical Approaches in Google Trends Research: Systematic Review. *Journal of Medical Internet Research.* 2018;11(e270). Retrieved from: `https://www.jmir.org/2018/11/e270/`

[3] Mellon J. Assessing Spurious Correlations in Big Search Data. *MDPI Journal of Computational Social Science.* 2022;5(1):15. Retrieved from: `https://www.mdpi.com/2571-9394/5/1/15`

[4] Bragazzi NL, et al. Confounding Effect of Undergraduate Semester-Driven Academic Internet Searches on Google Trends Data. *JMIR Infodemiology.* 2022;2(e34464). Retrieved from: `https://infodemiology.jmir.org/2022/2/e34464`

[5] Kurian SJ, et al. Need of care in interpreting Google Trends-based COVID-19 infodemiological study results: potential risk of false-positivity. *BMC Medical Research Methodology.* 2021;21(338). Retrieved from: `https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-021-01338-2`

[6] Deccan Chronicle. Fake PhD Student Busted After 2 Weeks Inside IIT-Bombay. June 2024. Retrieved from: `https://www.deccanchronicle.com/nation/fake-phd-student-busted-after-2-weeks-inside-iit-bombay-1888848`

[7] The420.in. The Smartest Cyber Criminal? PhD Holder and UPSC Trainer Arrested in 2.46 Crore Cyber Fraud. September 2025. Retrieved from: `https://the420.in/pune-university-fraud-phd-engineer-iit-bombay-scam/`

[8] Shiksha. IIT Placements – Know Highest Salary Package & Placement Process. Retrieved from: `https://www.shiksha.com/engineering/articles/iit-placements-know-highest-salary-package-placement-process-blogId-32047`

[9] Afternoon Voice. There Are Many Fake Degree Mills In India. Retrieved from: `https://www.afternoonvoice.com/there-are-many-fake-degree-mills-in-india.html`

[10] Integrity Indonesia. 36,000 Fake Degrees Sold: How One Scandal Shook India's Education System. Retrieved from: https://www.integrity-indonesia.com/blog/renowned-indian-university-sells-36000-fake-degrees/

[11] South China Morning Post. India's fake degrees: hundreds in Singapore, Malaysia, US, Canada left questioning qualifications. Retrieved from: https://www.scmp.com/week-asia/people/article/3123929/indias-fake-degrees-hundreds-singapore-malaysia-us-canada-left

[12] YourStory. The story of the Gurugram startup that busted IT firm CEO for furnishing fake IIT, IIM degrees. May 2019. Retrieved from: https://yourstory.com/2019/05/gurugram-startup-background-verification-fake-degree-iit-iim

[13] ED Times. Indian FinTech Influencer's Alleged Fake Degrees Unmasked On Social Media, Deletes Accounts. Retrieved from: https://edtimes.in/indian-fintech-influencers-alleged-fake-degrees-unmasked-on-social-media-deletes-accou

[14] Business Insider India. The curious case of 'fake' influencer Ravisutanjani Kumar shocks X users. Retrieved from: https://www.businessinsider.in/india/news/the-curious-case-of-fake-influencer-ravisutanjani-kumar-shocks-x-users/articleshow/103654758.cms

[15] News24online. IIT Bombay Student's ID Misused In Shocking Scam Targeting JEE Aspirants With Fake Leaked Papers. Retrieved from: https://news24online.com/india/iit-bombay-students-id-misused-in-shocking-scam-targeting-jee-aspirants-with-fake-leake
587687/

[16] Wikipedia. Indian Institutes of Technology. Retrieved from: https://en.wikipedia.org/wiki/Indian_Institutes_of_Technology

[17] Wikipedia. National Academic Depository. Retrieved from: https://en.wikipedia.org/wiki/National_Academic_Depository

[18] Wikipedia. DigiLocker. Retrieved from: https://en.wikipedia.org/wiki/DigiLocker

[19] AESC. The Growing Risk of Diploma Mills. Retrieved from: https://www.aesc.org/insights/magazine/article/growing-risk-diploma-mills

[20] ScienceDirect. Information-Seeking Behavior - an overview. Retrieved from: https://www.sciencedirect.com/topics/social-sciences/information-seeking-behavior

[21] Wikipedia. Google Trends. Retrieved from: https://en.wikipedia.org/wiki/Google_Trends

The End