Unraveling Cybercrime in India: A Fuzzy ISM Approach to Antecedents and Outcomes

Srijan Pateriya[1*], Pushkar Dubey[2] and Parul Dubey[3]
{srijanpateriya99@gmail.com[1], pushkardubey22@gmail.com[2], dubeyparul29@gmail.com[3]}

Department of Law, Dr. C.V. Raman University, Kota, Bilaspur 495113, Chhattisgarh, India[1]
Department of Management, Pandit Sundarlal Sharma (Open) University, Bilaspur 495009, Chhattisgarh, India[2]
Department of Computer Science and Engineering, Symbiosis International (Deemed University), Symbiosis Institute of Technology, Wathoda, Nagpur 440008, Maharastra, India[3]

Abstract. This research analyses the causes and effects of Cybercrime in India by conducting structured analysis using Fuzzy Interpretive Structural Modeling (Fuzzy ISM). It discusses how systemic dependencies among main variables including technology development, low cybersecurity awareness, digital divide, and institutional weakness influence the aggregate effect of the variables on cybercrime incidence and its outcome in society. Hierarchical ordering of the influences is disclosed, with reminder of technological progression, poor consciousness, and economic discrepancies serving as ground-level causes of vulnerabilities over cyber networks. These forces invariably increase the vulnerability to cybercrime, causing or intensifying psychic harm, large scale economic damage, real national security threats, and diminishing the goodwill of the public toward online space. The model suggested contributes to both concept and practice along with subsystem implication of building cybersecurity resilience in India.

Keywords: Cybercrime, Cybersecurity, India, Fuzzy ISM, Digital Trust, Cybercrime Antecedents, Cybercrime Outcomes, Structural Modeling**.**

1 Background of the Study

We are currently in the age of Digital India, marking a transformative shift in the nation's history. The digital revolution has significantly reshaped India's socio-economic culture, introducing unprecedented changes that have made life more connected, efficient, and inclusive. With over 800 million internet users, India now ranks among the leading digital nations in the world. This rapid digital expansion has brought about a wave of benefits, improving access to services, empowering citizens, and providing a platform for economic growth.

However, along with these advancements, the digital age has also brought about a rise in cyber vulnerabilities. As technology continues to penetrate every aspect of daily life, it presents an expanding attack surface for cybercriminals. These vulnerabilities often manifest in the form of cyber fraud, identity theft, and other malicious activities that threaten the security and privacy of both individuals and organizations. The increase in cybercrimes is further exacerbated by a lack of awareness among users, compounded by insufficient training for law enforcement to address the growing number of cyber threats effectively.

Moreover, socio-economic factors such as poverty and high unemployment rates contribute to the rise in cybercrime, as individuals in vulnerable situations may turn to illegal online activities as a means of livelihood. Additionally, India's laws and regulatory frameworks, although

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358072

evolving, often lag behind the rapid pace of cyber threats, creating challenges for prosecution and deterrence. The impact of cybercrime extends beyond financial loss, affecting individuals psychologically and eroding trust in digital platforms, which could undermine India's ambitious goals for digital growth.

This study aims to explore the interrelationship between technological growth, awareness, economic conditions, and institutional capability, and how these factors jointly influence the prevalence of cybercrimes in India. By applying methods like Fuzzy ISM, this research seeks to develop a comprehensive model to enhance India's cyber security resilience and guide future policy planning.

2 Objectives of the Study

1. To understand and analyse the antecedents of cybercrime spread in India.
2. To compare the net losses and the societal cost manifested by incidences of cybercrime.
3. To construct a model pattern that illustrates the layering and relational nature of the bursting and implications of cybercrime.
4. To use Fuzzy ISM to make clear the systemic relations within the identified parameters.
5. To offer policy-relevant analyses and suggestions with the objective of enhancing cybersecurity resilience in India.

3 Methodology

The study is a quantitative research by Fuzzy Interpretive Structural Modelling (Fuzzy ISM) technique. The procedure includes the following:

1. Variable definition: The variables were developed through a review of literature and opinions of experts, which included technological development, economic gaps, security awareness, cybercrime cases, psychological and economic consequences, threats to national security, and institutional capability.
2. AFSSIM:The inter-variable based on the degree of their impact was allocated by the experts memory of the fuzzy values (0-1).
3. Fuzzy Reachability Matrix (Fuzzy RM): Transformation of AFSSIM into Fuzzy RM by fuzzy transitive closure for inclusion of indirect and direct influences among variables.
4. Defuzzified Reachability Matrix: The fuzzy values in the matrix were defuzzified to crisp binary relationships, clearly identifying the influence routes in the model.
5. Level Partitioning: Variables were grouped into stratified levels as determined by their drivering and targetability powers (root-cause, mediator, and effect).
6. Conical Matrix and Digraph Design: additional improvement resulted in a visual representation (digraph) reflecting all direct and indirect relationships.

7. Final Structural Model: Development of an interpretative hierarchical model illustrating the path-flow from antecedents to outcomes that offers tactical implications towards enhancing cybersecurity.

3.1 Definitions of Variables in the Conceptual Framework on Cyber Crime in India

V1: Technological Growth: Technological growth refers to the rapid development and adoption of digital infrastructure, including increased internet penetration, mobile connectivity, and digital services, which, while beneficial, also expands the digital attack surface for cybercriminals. [9]

V2: Lack of Awareness and Training: This refers to the insufficient knowledge and preparedness among citizens and enforcement agencies regarding cyber threats, safe internet practices, and the use of cybersecurity tools, which increases vulnerability to attacks. [11]

V3: Economic Disparities: Economic inequality, poverty, and unemployment can drive individuals toward illegal online activities for financial gain, thereby contributing to the rise in cybercrime in economically disadvantaged settings. [2]

V4: Cybersecurity Awareness: Cybersecurity awareness is the understanding and application of safe practices online, such as password management, recognizing phishing attempts, and ensuring digital hygiene, which helps reduce vulnerability. [4]

V5: Perceived Vulnerability: This is the subjective feeling of being exposed to or at risk of cyberattacks. It is shaped by personal experience, awareness levels, and exposure to digital threats. [7]

V6: Motivation to Offend: Refers to internal and external factors, such as financial stress, social environment, or low risk of being caught, that push individuals towards engaging in cybercriminal acts. [2]

V7: Cyber Crime Incidence and Exposure: Denotes the frequency and type of cybercrimes experienced by individuals or institutions, such as data breaches, identity theft, ransomware attacks, and phishing. [5]

V8: Psychological Outcomes: Cybercrime victims often suffer from emotional and psychological issues such as anxiety, fear, depression, and trauma, which impact their quality of life and digital trust. [3]

V9: Financial Outcomes: These are the economic losses sustained by victims of cybercrime, which may include unauthorized transactions, fraud, theft of assets, or identity-based financial damage. [6]

V10: National Security Threats: Cyberattacks on critical infrastructure such as government portals, financial systems, defense databases, and nuclear facilities pose a serious threat to national security and data sovereignty. [8]

V11: Law Enforcement Capacity: This refers to the preparedness, resources, technical expertise, and institutional frameworks available to law enforcement agencies to detect, investigate, and prosecute cybercrimes effectively. [10]

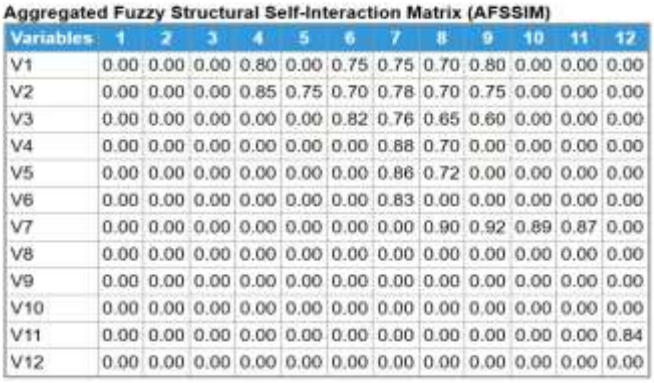
V12: Public Trust in Digital Platforms: Trust in digital systems such as online banking, e-governance, and e-commerce reflects citizens' confidence that these systems are secure, reliable, and transparent. High cybercrime rates erozdes this trust. [1]

4 Analysis and Interpretation

4.1 Fuzzy ISM-Based Analysis of Antecedents and Outcomes of Cyber Crime in India

The analysis employs Fuzzy Interpretive Structural Modelling (Fuzzy ISM) for exploring the interrelationships between the antecedents and causes of cybercrime in India. This methodology would enable identifying, ordering, and visualizing complex relationships among variables, with the aid of fuzzy logic to address the uncertainty and subjectivity in expert opinion.

The solution starts with the generation of the AFSSIM. Here, this matrix is to measure how much a variable contributes to the others with values between 0 and 1, providing a graded instead of binary matrix. For example, V2 (Lack of Awareness and Training) has a significant effect on V5 (Perceived Vulnerability) and V6 (Motivation to Offend), and V1 (Technological Growth) affects V4 (Cybersecurity Awareness) and V5. These relationships are validated using expert consensus and literature review. Fig. 1 shows the Adjacency Fuzzy Structural Self-Interaction Matrix (AFSSIM).

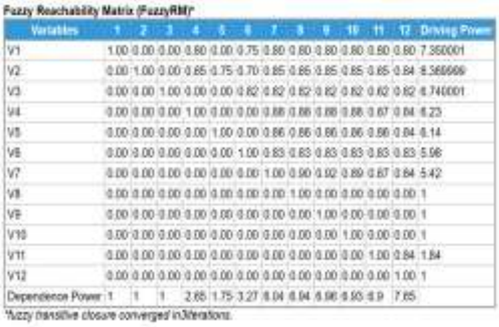


Aggregated Fuzzy Structural Self-Interaction Matrix (AFSSIM)

Variables	1	2	3	4	5	6	7	8	9	10	11	12
V1	0.00	0.00	0.00	0.80	0.00	0.75	0.75	0.70	0.80	0.00	0.00	0.00
V2	0.00	0.00	0.00	0.85	0.75	0.70	0.78	0.70	0.75	0.00	0.00	0.00
V3	0.00	0.00	0.00	0.00	0.00	0.82	0.76	0.65	0.60	0.00	0.00	0.00
V4	0.00	0.00	0.00	0.00	0.00	0.00	0.88	0.70	0.00	0.00	0.00	0.00
V5	0.00	0.00	0.00	0.00	0.00	0.00	0.86	0.72	0.00	0.00	0.00	0.00
V6	0.00	0.00	0.00	0.00	0.00	0.00	0.83	0.00	0.00	0.00	0.00	0.00
V7	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.90	0.92	0.89	0.87	0.00
V8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
V9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
V10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
V11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.84
V12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Fig. 1. Adjacency Fuzzy Structural Self-Interaction Matrix (AFSSIM).

Once the AFSSIM is constructed, the next step involves converting it into the Fuzzy Reachability Matrix (FuzzyRM) using fuzzy transitive closure operations (see Fig 2). This matrix captures all direct and transitive influences among variables. Driving and dependence powers are computed in this step. Variables such as V2 (driving power = 8.38) and V1 (driving power = 7.35) emerge as strong influencers, whereas V8, V9, and V10 exhibit high dependence, indicating their status as final outcomes.



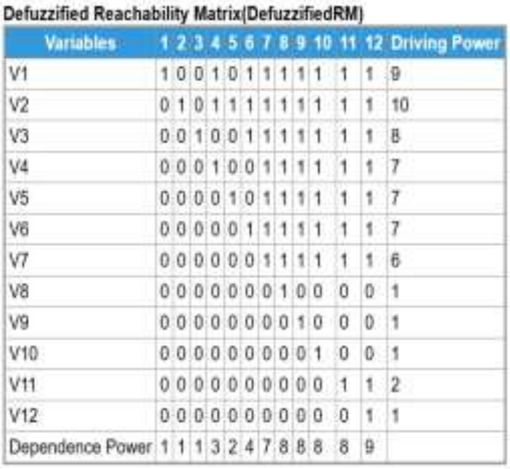
Fuzzy Reachability Matrix (FuzzyRM)*

Variables	1	2	3	4	5	6	7	8	9	10	11	12	Driving Power
V1	1.00	0.00	0.00	0.80	0.00	0.75	0.80	0.80	0.80	0.80	0.80	0.80	7.350001
V2	0.00	1.00	0.00	0.85	0.75	0.70	0.85	0.85	0.85	0.85	0.85	0.84	8.368666
V3	0.00	0.00	1.00	0.00	0.00	0.82	0.82	0.82	0.82	0.82	0.82	0.82	6.740001
V4	0.00	0.00	0.00	1.00	0.00	0.00	0.88	0.88	0.88	0.88	0.87	0.84	6.23
V5	0.00	0.00	0.00	0.00	1.00	0.00	0.86	0.86	0.86	0.86	0.86	0.84	6.14
V6	0.00	0.00	0.00	0.00	0.00	1.00	0.83	0.83	0.83	0.83	0.83	0.83	5.98
V7	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.90	0.92	0.89	0.87	0.84	5.42
V8	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	1
V9	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	1
V10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	1
V11	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.84	1.84
V12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	1
Dependence Power	1	1	1	2.65	1.75	3.27	6.04	6.94	6.96	6.93	6.9	7.65	

*fuzzy transitive closure converged in3iterations.

Fig. 2. Fuzzy Reachability Matrix (Fuzzy RM).

To enhance interpretability, the fuzzy values are transformed into binary form in the Defuzzied Reachability Matrix (see Fig 3). This transformation enables a crisp representation of relationships, making it easier to identify which variables influence others. The defuzzification threshold is applied based on expert-defined criteria, and the matrix is used to compute updated driving and dependence power scores. These scores directly inform the hierarchical ordering of variables.

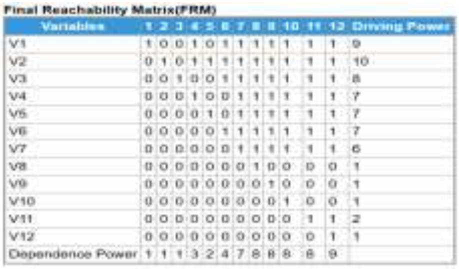


Defuzzified Reachability Matrix(DefuzzifiedRM)

Variables	1	2	3	4	5	6	7	8	9	10	11	12	Driving Power
V1	1	0	0	1	0	1	1	1	1	1	1	1	9
V2	0	1	0	1	1	1	1	1	1	1	1	1	10
V3	0	0	1	0	0	1	1	1	1	1	1	1	8
V4	0	0	0	1	0	0	1	1	1	1	1	1	7
V5	0	0	0	0	1	0	1	1	1	1	1	1	7
V6	0	0	0	0	0	1	1	1	1	1	1	1	7
V7	0	0	0	0	0	0	1	1	1	1	1	1	6
V8	0	0	0	0	0	0	0	1	0	0	0	0	1
V9	0	0	0	0	0	0	0	0	1	0	0	0	1
V10	0	0	0	0	0	0	0	0	0	1	0	0	1
V11	0	0	0	0	0	0	0	0	0	0	1	1	2
V12	0	0	0	0	0	0	0	0	0	0	0	1	1
Dependence Power	1	1	1	3	2	4	7	8	8	8	8	9	

Fig. 3. Defuzzified Reachability Matrix.

The Final Reachability Matrix (FRM) (see Fig 4) refines the structure by validating the strongest, most significant relationships. This matrix confirms the consistent directional influences and prepares the ground for level partitioning. Here, variables with high driving power but low dependence (such as V1–V3) are positioned as root causes, while those with high dependence but low driving power (like V8–V12) are considered end outcomes.

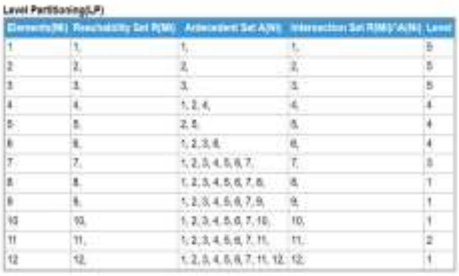


Final Reachability Matrix(FRM)

Variables	1	2	3	4	5	6	7	8	9	10	11	12	Driving Power
V1	1	0	0	1	0	1	1	1	1	1	1	1	9
V2	0	1	0	1	1	1	1	1	1	1	1	1	10
V3	0	0	1	0	0	1	1	1	1	1	1	1	8
V4	0	0	0	1	0	0	1	1	1	1	1	1	7
V5	0	0	0	0	1	0	1	1	1	1	1	1	7
V6	0	0	0	0	0	1	1	1	1	1	1	1	7
V7	0	0	0	0	0	0	1	1	1	1	1	1	6
V8	0	0	0	0	0	0	0	1	0	0	0	0	1
V9	0	0	0	0	0	0	0	0	1	0	0	0	1
V10	0	0	0	0	0	0	0	0	0	1	0	0	1
V11	0	0	0	0	0	0	0	0	0	0	1	1	2
V12	0	0	0	0	0	0	0	0	0	0	0	1	1
Dependence Power	1	1	1	3	2	4	7	8	8	8	8	9	

Fig. 4. Final Reachability Matrix (FRM).

Using the FRM, the Level Partitioning Table is generated (see Fig 5). This step organizes the variables into hierarchical levels based on their reachability and antecedent sets. The results show that V1 (Technological Growth), V2 (Lack of Awareness), and V3 (Economic Disparities) form Level 5, signifying root causes. V4, V5, and V6, which mediate exposure to cybercrime, occupy Level 4. Cybercrime exposure (V7) is placed at Level 3, while law enforcement capacity (V11) is positioned at Level 2, followed by the most dependent variables psychological outcomes, financial losses, national security threats, and public trust (V8–V10, V12) in Level 1.

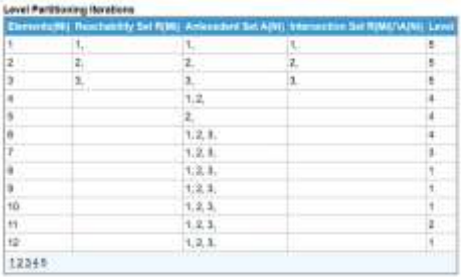


Level Partitioning(LP)

Elements(Mi)	Reachability Set R(Mi)	Antecedent Set A(Ni)	Intersection Set R(Mi)^A(Ni)	Level
1	1,	1,	1,	5
2	2,	2,	2,	5
3	3,	3,	3,	5
4	4,	1, 2, 4,	4,	4
5	5,	2, 5,	5,	4
6	6,	1, 2, 3, 6,	6,	4
7	7,	1, 2, 3, 4, 5, 6, 7,	7,	3
8	8,	1, 2, 3, 4, 5, 6, 7, 8,	8,	1
9	9,	1, 2, 3, 4, 5, 6, 7, 9,	9,	1
10	10,	1, 2, 3, 4, 5, 6, 7, 10,	10,	1
11	11,	1, 2, 3, 4, 5, 6, 7, 11,	11,	2
12	12,	1, 2, 3, 4, 5, 6, 7, 11, 12,	12,	1

Fig. 5. Level Partitioning Table.

The Level Partitioning Iterations Table (see Fig 6) shows how variables are iteratively assigned levels until all are sorted based on their influence structure. This table tracks the movement of variables from raw form to refined hierarchical levels across iterations.

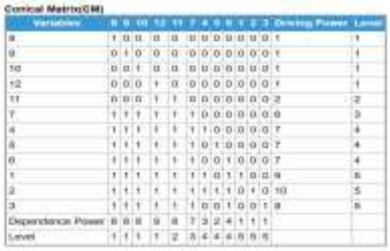


Level Partitioning Iterations

Elements(Mi)	Reachability Set R(Mi)	Antecedent Set A(Ni)	Intersection Set R(Mi)^A(Ni)	Level
1	1,	1,	1,	5
2	2,	2,	2,	5
3	3,	3,	3,	5
4		1, 2,		4
5		2,		4
6		1, 2, 3,		4
7		1, 2, 3,		3
8		1, 2, 3,		1
9		1, 2, 3,		1
10		1, 2, 3,		1
11		1, 2, 3,		2
12		1, 2, 3,		1
1 2 3 4 5				

Fig. 6. Level Partitioning Iterations Table.

The structure is then reorganized using the Conical Matrix (CM) (see Fig 7), which clusters variables by their final levels and directional influence. This matrix presents a condensed visualization of influence flows across levels. Driving and dependence powers are clearly shown, and the structure aligns with logical progression from root causes to systemic outcomes.



Conical Matrix(CM)

Variables	8	9	10	12	11	7	4	5	6	1	2	3	Driving Power	Level
8	1	0	0	0	0	0	0	0	0	0	0	0	1	1
9	0	1	0	0	0	0	0	0	0	0	0	0	1	1
10	0	0	1	0	0	0	0	0	0	0	0	0	1	1
12	0	0	0	1	0	0	0	0	0	0	0	0	1	1
11	0	0	0	1	1	0	0	0	0	0	0	0	2	2
7	1	1	1	1	1	1	0	0	0	0	0	0	6	3
4	1	1	1	1	1	1	1	0	0	0	0	0	7	4
5	1	1	1	1	1	1	0	1	0	0	0	0	7	4
6	1	1	1	1	1	1	0	0	1	0	0	0	7	4
1	1	1	1	1	1	1	1	0	1	1	0	0	9	5
2	1	1	1	1	1	1	1	1	1	0	1	0	10	5
3	1	1	1	1	1	1	0	0	1	0	0	1	8	5
Dependence Power	8	8	8	9	8	7	3	2	4	1	1	1		
Level	1	1	1	1	2	3	4	4	4	5	5	5		

Fig. 7. Conical Matrix.

The Digraph (see Fig 8) offers a comprehensive visual of all directed relationships in the system. The dense network confirms the interconnectivity between various drivers and outcomes, with particular emphasis on central nodes such as V7 (Cybercrime Exposure) acting as pivotal intermediaries.

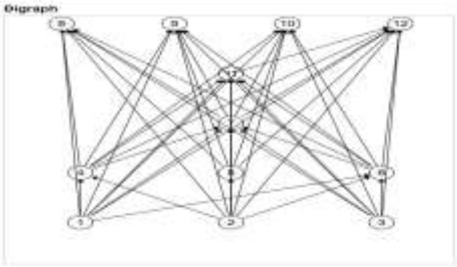


Fig. 8. Digraph of Variable Relationships.

Finally, the Final Model (see Fig 9) illustrates a simplified, hierarchically organized representation of the conceptual structure. The model starts with base variables (V1–V3) at the bottom, progresses through mediators (V4–V6), and leads to cybercrime exposure (V7), which cascades into outcomes (V8–V12). This figure provides the clearest strategic map for interpreting the directional flow from antecedents to consequences in the context of cybercrime.

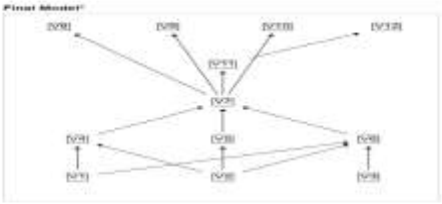
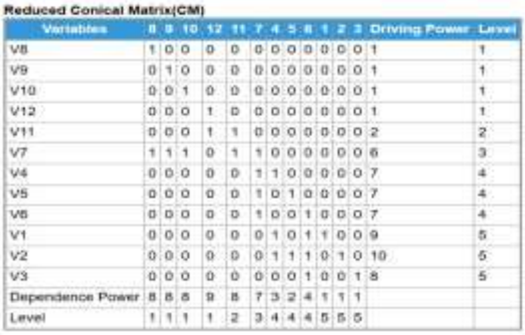


Fig. 9. Final Interpretive Structural Model.

The Reduced Conical Matrix (CM) (see Fig 10) confirms this structure with a focused matrix that filters out redundant relationships and strengthens the final interpretive diagram. The final model based on the substitution and relationship among the variables is presented in fig 11.



Reduced Conical Matrix(CM)

Variables	8	9	10	12	11	7	4	5	6	1	2	3	Driving Power	Level
V8	1	0	0	0	0	0	0	0	0	0	0	0	1	1
V9	0	1	0	0	0	0	0	0	0	0	0	0	1	1
V10	0	0	1	0	0	0	0	0	0	0	0	0	1	1
V12	0	0	0	1	0	0	0	0	0	0	0	0	1	1
V11	0	0	0	1	1	0	0	0	0	0	0	0	2	2
V7	1	1	1	0	1	1	0	0	0	0	0	0	6	3
V4	0	0	0	0	0	1	1	0	0	0	0	0	7	4
V5	0	0	0	0	0	1	0	1	0	0	0	0	7	4
V6	0	0	0	0	0	1	0	0	1	0	0	0	7	4
V1	0	0	0	0	0	0	1	0	1	1	0	0	9	5
V2	0	0	0	0	0	0	1	1	1	0	1	0	10	5
V3	0	0	0	0	0	0	0	0	1	0	0	1	8	5
Dependence Power	8	8	8	9	8	7	3	2	4	1	1	1		
Level	1	1	1	1	2	3	4	4	4	5	5	5		

Fig. 10. Reduced Conical Matrix.

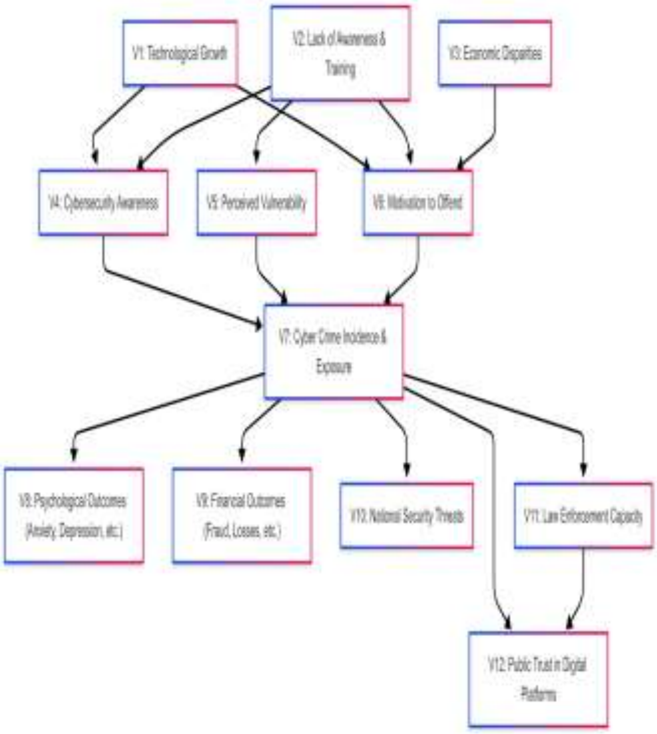

V1: Technological Growth
V2: Lack of Awareness & Training
V3: Economic Disparities
V4: Cybersecurity Awareness
V5: Perceived Vulnerability
V6: Motivation to Offend
V7: Cyber Crime Incidence & Exposure
V8: Psychological Outcomes (Anxiety, Depression, etc.)
V9: Financial Outcomes (Fraud, Losses, etc.)
V10: National Security Threats
V11: Law Enforcement Capacity
V12: Public Trust in Digital Platforms

Fig. 11. Final Model based on Substitution Relationships.

Altogether, the employment of Fuzzy ISM allows formulating a transparent, data-centric, and hierarchical structured view on how cybercrime is driven in India through its basal drivers and how is it resulting into the multi-dimensional outcomes. This model offers both theoretical understanding and pragmatic advice for policymakers, cyber security professionals and educators as the over-arching criticality to enhance root-level factors like awareness, financial capacity and digital skills to lessen the broader social consequences of cybercrime.

5 Discussions

The objective of this study was to understand the complex nature of cybercrime and to explore the deep and severe extent of its critical root and societal consequences in an Indian context which is being realized through the usage of Fuzzy Interpretive Structural Modelling (Fuzzy ISM). Several key observations and implications are highlighted by the empirical results from the hierarchical model.

First, the underlying assumption of technological expansion being a catalyst in the growth of cybercrime which has been a traditional stance is supported by current literature on the flip side of digital progress (Kethineni, 2020). “Adding them to a growing pool of targets”: fast progressing technology had certainly broadened economic and social inclusion, while also broadening vulnerabilities: there are increasingly more digital endpoints that can be leveraged for cyber threats. Accordingly, while digital infrastructure increases in number, aggressive cybersecurity attempts should accompany this trend, which, at present, seems to be lacking.

Further the study´s recognition of lack of awareness as another primary antecedent also finds strong empirical support from earlier re-search that of Singh (2023) and chugh et al. (2023). Despite major investments in digital literacy, awareness on the good practices of cybersecurity is dangerously low among the general population and, even worse, in law enforcement law enforcement presiding over the fight against cybercrime. This lack of knowledge plays a major role in increasing people’s perceived threat to make them feel more vulnerable to crimes, therefore enhancing the chances for people to engage in cybercrimes. Hence it is important to focus on targeted training programmes which should focus not only on making the public aware on but also (b) on improving the technical skills of cyber security enforcement units.

Economic inequalities and poverty, or an inability to obtain a minimum standard of living among people, are other important underlying factors against the landscape of which the upsurge in cybercrime needs to be seen. Al-Suwaidi et al. (2018) pointed out that financial difficulties, poverty, and unemployment could encourage cybercrime as a financial solution in daily life. This contention is well supported by the present model which implies that effective combating of cybercrime requires not only security but social and economic reforms in the form of reducing income disparity, and creating legitimate work for the deprived population.

The fuzzy ISM based hierarchical framework distinctly highlights mediating constructs that involve the conversation between cybersecurity awareness, perceived vulnerability and motivation to offend. This three-way interaction plays an intermediary role on the association between root-level drivers and cybercrime exposure outcome. Awareness of cybersecurity is a factor reducing perceived vulnerability, which, in turn, would reduce the likelihood that an individual falls a victim. Similarly, it is also found that sustained vulnerability and incentives were significant in increasing the likelihood of experiencing cybercrime, therefore verifying Herode (2020) and Al-Suwaidi et al. s’ (2018) prior findings that psychological factors are highly motivating in criminality.

At the outcomes level, the research identified significant psychological, financial, and national security impacts that break down-the alight public trust in digital systems. The high prevalence of psychological diseases including anxiety, trauma and depression as observed by Balabantaray (2024) drastically decreases the societal readiness for digitalisation in addition to the general trend of digital despondency in India, which curbs the broader digital transformation efforts in India. Monetary losses, especially in a developing digital economy such as India, would not only harm the gullible victims, but also pose severe challenges to economic situation, which is a similar worry that has been raised by Godbole et al. (2022).

Of significance, the threats to national security identified by cybercrime also illustrate the necessity of strong cyber security structures within governments and institutions, a fact reinforced by Hussain et al. (2023). Cyber-threats to critical national infrastructure demand policy makers' urgent, pragmatic focus for securing essential systems that are crucial to security and economic vitality.

Thirdly, reduced public trust in digital platforms is perhaps the most pervasive societal consequence. For example, trust is a network bed-rock for engaging in the digital space in e-governance, online banking, and commerce (Afzal et al., 2024). The study further points out that continuance of high rates of cybercrime seriously breach this trust leading to possible failures in the digitisation agenda of India that is aiming towards long-term developmental goals.

From a methodological standpoint, the use of Fuzzy ISM resulted in a robust and subtle view of complex interdependencies between variables. The application of fuzzy logic sufficiently reflected expert subjectivity and uncertainty, ultimately improving the reliability and validity of the insights gained.

6 Recommendations

The recommendations that can be derived from the rich findings of this research is:

a) Design and establish integrated cybersecurity awareness programs directed at citizens and law enforcement to identify and manage threats proactively.

b) Put in place inclusive economic development measures to address social-economic conditions that are drivers of motivation foe cybercrime.

c) Enhance legal instruments and enforcement capabilities, statutory regime should be made flexible so that laws keep pace with emerging cyber threats.

d) Expand national cybersecurity infrastructure to safeguard critical systems and restore public confidence in digital environments.

7 Implications and Scope for Further Research

The present study has important theoretical and practical implications, providing a structured comprehension of cybercrime-inclined dynamics as well as its societal ramifications in India.

Theoretical Implications:

- The Fuzzy ISM based hierarchical model contributes to the existing literature by specifying the relations among technological, social-economic and institutional antecedents and their effects in a better way.
- It adds to the cybercrime libraries, for example by utilising fuzzy logic to accommodate to fuzzy and subjective reasoning providing fine grained understanding in regard to these matters that traditional analytical frameworks can't afford to obtain not digest.

Practical Implications:

- Our findings can help guide cybersecurity investment by policymakers including dealing with technology vulnerabilities, awareness campaigns and economic inequality.
- Schools can produce tailored curriculums related to digital awareness and preparedness for cybersecurity in order to minimize society's susceptibility to cyber risk.
- These findings can be also used by LE/CS professionals to optimise training and operations, such as focusing on the root causes and fortifying response.

Scope for Further Research:

- Further research could also enhance the model by introducing other factors including international cooperation in cyberspace, new technologies (ICTs, artificial intelligence, blockchain) and new practices of cybersecurity.
- Longitudinal approaches to the data would yield important information about how these relationships change with time, given the fast pace of technology and cybercrime tactics.
- Cross-comparisons in terms of geographical areas and sectors (i.e., banking, health, and public governance) can also strengthen and extend the generalisability of our model.

8 Conclusions

This study provides a holistic analysis of the precedents and consequences for cybercrime in India by a systematic utilization of the Fuzzy Interpretive Structural Modelling (Fuzzy ISM). The results demonstrate a strong ordered structure among the variables; technological development, the lack of awareness of cybersecurity, and continuing of economic inequalities were all identified as the crucial basic causes of the cybercrime vulnerability. These are the root level causes of cybercrime problem, which contributes heavily in causing severe psychological…impact, huge economic losses, national threat, public distrust towards electronic platform.

The study highlights the intricate nature of cybercrime dynamics and the necessity for multidimensional solutions. Strategic implications suggest a need for integrated effort on policy strengthening, smart cyber security framework, inclusive digital literacy programme and socio-economic transformation. India has an opportunity to proactively address root antecedents and build more cyber security resilience to promote sustainable digital growth and socio-economic stability.

9 Limitations of the Study

Although a major contribution is made by this study, the authors note several limitations:

a) Expert Subjectivity of Judgments: Despite uncertainty being considered in fuzzy logic, subjective viewpoints in assessments provided by experts may be biasing or remain incomplete, subsequently leading to the credibility of the relationship between variables.

b) Cross-sectional: The present study provides a snapshot in time of cybercrime dynamics; as such it does not provide a view of how shifts in time and long-term cyber trends/ response trends occur.

c) Generalizability of Findings: The specific concentration on an Indian perspective as an example, may limit the ability to generalize the results of this study to other parts of the world with different economic, social and technical possibilities.

d) Limitation on Variables' Scope: Although the model embraces key variables including literature and expert opinion, other variables such international cybersecurity governance, technology development, and transboundary cyber threats are not accounted for.

References

[1] Afzal, M., Ahmad, N., & Ansari, M. S. (2024). Effect of cyberfraud and cybersecurity awareness on usage intention of e-banking users in India. In Responsible Production and Consumption-Agricultural Sustainability and Food Security.

[2] Al-Suwaidi, N., Nobanee, H., & Jabeen, F. (2018). Estimating causes of cybercrime: Evidence from panel data FGLS estimator. International Journal of Cyber Criminology, 12(1), 131–145.

[3] Balabantaray, S. R. (2024). Examining the impact of cyber fraud on Indian society: An assessment of the potential damage. In Cybersecurity, Law, and Economics: The Case of India.

[4] Chugh, M., Chugh, N., & Akhtar, A. (2023). Cybersecurity insights in software development organisations: An empirical study in India. International Journal of Business Information Systems, 44(1), 1–20.

[5] Diya, C. R., Umme Salma, M., & Beerannavar, C. R. (2023). A case study on zonal analysis of cybercrimes over a decade in India. In Cybersecurity for Decision Makers, 29–46.

[6] Godbole, T., Gochhait, S., & Ghosh, D. (2022). Developing a framework to measure cyber resilience behaviour of Indian bank employees. Smart Innovation, Systems and Technologies, 274, 231–241.

[7] Herode, P. J. (2020). Cybercrime vis-à-vis violation of massive human rights and legislative efficacy in India. Indian Journal of Law and Justice, 11(2), 110–128.

[8] Hussain, S., Ashraf, S., Seep, (...), & Ul Abideen, Z. (2023). A critical analysis on cybercrimes. In 2nd International Conference on Business Analytics for Technology and Security (ICBATS 2023).

[9] Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. In the Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 705–726). Palgrave Macmillan.

[10] Mohapatra, D. (2022). Cyber security legal framework in India: An appraisal. In Cross-Industry Applications of Cyber Security Frameworks, 94–109.

[11] Singh, D. (2023). Emerging trends in cybercrimes. In Sustainable Business and IT, 111–128.