Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 4, October-2023, ISSN 2230-7540

Evolution and impact of Cybercrimes in India: Trends, Patterns, and Socio-Economic Implications

S. Nakkeeran[1]*, Dr. Dharamveer Singh[2]

[1] Research Scholar, University of Technology, Jaipur, Rajasthan, India

Email: advocatekeeran@gmail.com

[2] Associate Professor, Dept.of Law, University of Technology, Jaipur, Rajasthan, India

Abstract - The patterns, trends, and effects of cybercrimes on the financial sector are the subject of this research. A thorough understanding of the nature and effects of financial cybercrimes is necessary since these crimes constitute serious dangers to people, companies, and governments. Cybersecurity experts, lawmakers, and law enforcement can better protect financial systems, organisations, and people from cyberattacks if they study the methods hackers use to compromise these systems. Significant monetary losses, diminished faith in online transactions, and interruptions to essential infrastructure and services are some of the far-reaching effects of financial cybercrimes on the economy. Beyond the obvious monetary losses, these effects ripple via investment choices, customer trust, and productivity. Financial cybercrimes may have a significant economic effect; stakeholders need to invest in cybersecurity, strengthen authentication mechanisms, and raise cybersecurity awareness to mitigate this. To further discourage cybercriminals and enable coordinated reactions to cybercrimes that span international borders, thorough rules and international collaboration are required. It takes a look at the many forms of cybercrime in India, the damage they do, and the steps the government and others have done to stop them. In addition to outlining possible solutions to lessen the impact of cybercrime, the paper emphasises the difficulties in doing so.

Keywords: Cyber-crimes, Economic, Cyberspace, crime, prevention models.

----------X----------

INTRODUCTION

Numerous facets of modern life and business have been profoundly affected by the explosion of internet use and other forms of fast-moving information technology in the last few years. While these advancements have undoubtedly improved many aspects of life, they have also introduced new threats, most notably cybercrime. The term "cybercrime" describes any kind of unlawful activity that targets people, businesses, or even governments via the use of computer systems or networks. The country's hackers have set their sights on India because of its thriving economy and growing dependence on digital technology. Cybercriminals have found a welcoming environment in the nation thanks to its big population, increasing internet usage, and developing digital infrastructure. The significance of comprehending the effects of cybercrime on Indian society and the economy cannot be overstated.

Definition of Cybercrime:

Crimes perpetrated via the use of computers, computer networks, or the internet are collectively known as cybercrime. These types of crimes take use of security holes in computer networks to damage people, businesses, or governments via gaining unauthorised access, stealing sensitive data, or interrupting services.

Some common types of cybercrime include:

a. **Hacking**: Breaking into computer systems or networks without authorization in order to steal, modify, or delete data, interrupt services, or initiate more assaults.

b. **Identity Theft:** Theft of personally identifiable information (PII) by unauthorised parties for the purpose of impersonation or fraud.

c. **Social engineering and phishing:** fooling someone into giving up personal information or carrying out a desired activity via the use of misleading electronic communication.

d. **Attacks using Malware:** The dissemination of programmes with harmful intent, such as viruses, worms, or ransomware, in order to breach systems, steal data, or demand ransom.

e. **Financial Fraud:** using internet frauds, credit card fraud, or crimes pertaining to cryptocurrencies in order to illicitly acquire financial benefits.

f. **Data Breaches:** When private information, such customer records or company secrets, falls into the wrong hands, it may cause privacy breaches or even abuse.

g. **Cyberbullying and Harassment:** Assaults, threats, and harassment perpetrated by electronic means, most often via social media and messaging applications.

h. **Cyber espionage:** the wrongdoing of hackers or state-sponsored organisations with the aim of obtaining confidential data or interfering with official government operations. Cybercrime Trends Worldwide:

As a result of its proliferation and pervasiveness, cybercrime has become an international problem. Some important worldwide tendencies in cybercrime are:

i. **Growing Complexity:** Cybercriminals are always coming up with new ways to strike, using new technology and strategies to make their assaults more targeted and complex.

j. **Ransomware Attacks:** Cybercriminals encrypt victims' data and demand ransom payments to decrypt it. Ransomware has become a common danger.

k. **Illicit Trade on the Dark Web:** Stolen information, hacking tools, narcotics, and firearms are all for sale on this clandestine marketplace.

l. **Attacks on the Supply Chain:** In order to steal sensitive information or bring down reliable systems, cybercriminals aim their attacks at weak points in the supply chain.

m. **Security Flaws in the Internet of Things (IoT):** Hackers now have more ways than ever to get unauthorised access by exploiting security holes in the ever-growing network of interconnected devices.

n. **Attacks Sponsored by States:** Governments conduct cyber espionage, sabotage, or disruptive operations for the purpose of advancing national objectives or gaining a geopolitical advantage.

LITERATURE REVIEW

Gourav Singh (2023), This study investigates the ever-changing scene of cybercrime in India, looking at the patterns, obstacles, and solutions that have been implemented to combat it. Cybercrime has increased in recent years in India, threatening not just people and businesses but also the country's cyber security infrastructure, thanks to the proliferation of digital technology. This article describes the several forms of cybercrime that occur in India, discusses the causes of their proliferation, outlines the country's regulatory frameworks and law enforcement initiatives, and concludes with recommendations for improving cyber defences. The relevance of cybercrime in India is first discussed in this abstract. It describes the many forms of cybercrime and the variables that have led to its proliferation. In addition to discussing the business sector's and government's efforts to fight cybercrime, the abstract delves into the regulatory and legislative framework, the difficulties faced by law enforcement, and the steps taken to mitigate these issues in India. Future trends and rising cybercrime concerns in India are also highlighted, along with the significance of international collaboration. Additionally, it covers the suggestions for enhancing India's cyber defences.

“Nir Kshetri.” (2016) India is seeing a dramatic increase in cybercrime. India and other developing economies are particularly vulnerable to cybercrime. The topic of cybersecurity and cybercrime in India is explored in this study. This study draws on a wide range of sources, including the writings of researchers in the fields of economics, criminology, institutional theory, and international relations. We analyse the cybercrime and cybersecurity situations in India using a framework that outlines the links between official and informal institutions, diverse sources of wealth and poverty, and elements linked to international relations and cybercrime and cybersecurity. Cybercrime and cybersecurity in poor nations are impacted by developmental, institutional, and international relations concerns, according to the results.

This is a research article from 2023 by Chen, Hao, Ding, Jiang, Dong, Zhang, Guo, and Gao. The worldwide economy, social stability, national security, and personal interests are all being negatively impacted by cybercrime. Presently,

technological countermeasures are the main emphasis of cybercrime mitigation efforts. Taking cybercrime into account as a social phenomena, this research builds a theoretical framework that incorporates cybercrime-influencing social, economic, political, and technical aspects. To create a global map of subnational cybercrimes, researchers utilise the innovative cybersecurity data collection known as the FireHOL IP blocklist. To determine which variables have the most impact on cybercrime, researchers utilise generalised linear models (GLMs). To quantify the direct and indirect impacts of these factors, structural equation modelling (SEM) is used. Although the impacts of socioeconomic development on cybercrime vary by income level, the GLM findings imply that include a wide range of socioeconomic parameters might greatly enhance the model's explanatory power. Cybercrime is directly linked to socioeconomic development. Technological aspects mediate the association between socioeconomic circumstances and cybercrime, according to SEM findings, which show that cybercrime is causally related to a wide range of contextual factors.

Khan, N.F., Ikram, N. & Saleem, S. (2023), Cybersecurity risks are a growing concern in developing nations as more and more educational activities move online. When seen through the prism of the stratification model of technology spread, digital knowledge and skills serve to perpetuate existing social and digital gaps. Socioeconomic and digital disparities, especially in developing countries, impact cybersecurity, a digital competency.

This research uses a face-to-face survey to investigate the cybersecurity behaviours of students enrolled in higher education institutions (HEIs) throughout Pakistan. It fills the gap in empirical information about digital divide in terms of cybersecurity. Seven hundred and fifty-eight people from economically and geographically diverse cities throughout the nation were selected using a multi-stage stratified selection approach. We used descriptive statistics and Pearson's Chi-square to analyse the data.

The findings demonstrate that students' cybersecurity practices on mobile devices are lacking. The cybersecurity behaviours of pupils varied significantly across socioeconomic and digital gap characteristics. People from lower socioeconomic backgrounds and those with less internet access are more likely to be victims of cybercrime. The study's findings highlight the need for kids from disadvantaged backgrounds to get individualised cybersecurity education programmes that address digital divide.

By 2022, Ho and Luong had To fill this knowledge vacuum, our study combed through the Web of Science database from 2010 to 2020 for 387 Social Science Citation Index papers that dealt with cybercrime victimisation. This article's goal is to scour the literature for patterns in research and publishing patterns broken down into five categories: time, prolific authors, notable sources, active institutions, and top countries/regions.

Cybercrime victimisation research gaps and worldwide cooperation are other objectives of this study. The results showed a clear rising trend in the number of publications throughout that time. In the field of cybercrime victimisation research, the United States, its authors, and its institutions certainly had extensive connections and had a pivotal role.

Over the years, cyberbullying has emerged as the leading worry, with cyber interpersonal crimes receiving more attention than internet-dependent crimes. It is recommended that future studies focus more on older adults and gather data from a variety of nations, not only those in Europe or the United States. There should be more cross-national research in less-visited continents on the research map. This study helped academics optimise their own research directions, provided statistical data and graphic results to provide an overview of the scholarly state of cybercrime victimisation, and encouraged authors and institutions in developing methods for research cooperation.

Analysis of the Study

Rate of Growth of Cyber Crime in India

This section deals with the rate of growth of cybercrime in India. In order to analyze the rate of cybercrime in India, we used regression analysis and the results of the test are the following (Table 1) (Figure 1)

What you see here is the result of an Exponential model statistical regression test, where the dependent variable was compared to one independent variable. A breakdown of the findings is shown here:

The R-squared value: This number indicates the extent to which the independent variable in the model can account for the variation in the dependent variable. A high level of correlation between the two sets of data is shown by the exponential model's R Squared score of 0.981. The F-test determines the model's overall significance, and this number represents the outcome. The exponential model is important and may give helpful information, as shown by the 907.913 F value, which is statistically significant.

Values for df1 and df2 indicate the model's degrees of freedom. The two variables that make up a dependent variable are the number of observations and the number of independent variables, which are denoted as df1 and df2, respectively. Df1 is 1 and df2 is 18 in the exponential model.

Table 1. Model Summary and Parameter Estimates (India).

Dependent Variable: India							
Model Summary						Parameter Estimates	
Equation	square	F	df1	df2	Sig.	constant	b1
Exponential	.981	907.913	1	18	<.001	11.778	.407

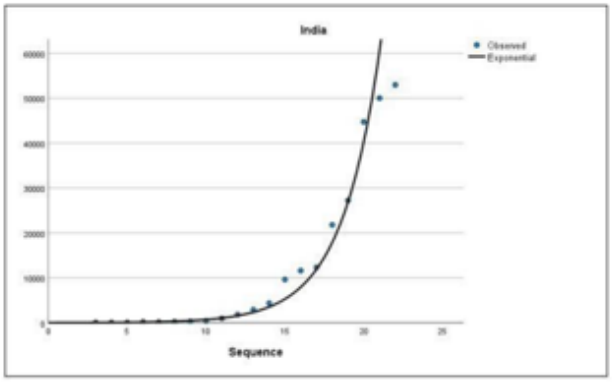

Figure 1. Rate of Growth of Cyber Crime in India.

Sig: The F-test significance level is represented by this value. At the 95% confidence level, the exponential model is noteworthy since its Sig value is smaller than 0.05.

These numbers represent the parameter estimations for the model's independent variable's intercept and coefficient: constant and b1. The Exponential model has the numbers 11.778 and 0.407. These numbers tell us something about the connection between the two variables, the independent and dependent ones.

Trends of Cyber Crime in India and the USA

Cybercrime trends in the US and India are discussed in this section. The trend analysis is based on data collected from the Internet Crime Report and the Crime in India report. Figure 2 shows the results of the trends in cybercrime.

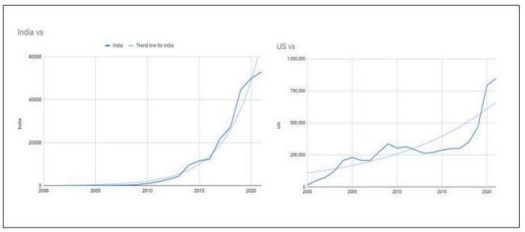

Figure 2. Rate of Growth of Cyber Crime in India and the USA.

It is clear from the graph that there is a critical moment when the structure breaks. A Wald test was conducted to have a better understanding of the specifics of a structural breach. When there is a major shift in the fundamental structure of time series data, it is called a structural break. Several things, such shifts in economic policy, natural calamities, or new technologies, might bring about this transformation, which can be either rapid or slow. Time series data analysis and forecasting are both impacted by structural breakdowns, which alter the connections between variables and undermine the accuracy of statistical models. So, when looking at time series data, it's crucial to find structural fractures and take them into consideration. To find out whether there is a structural break in time series data, statisticians apply the Wald test. It checks for statistical differences between the estimated model parameters before and after a given time point. A structural breach has occurred if the test shows that the estimations are significantly different. When doing econometric research, the Wald test is often used to identify when economic linkages have changed over time. Because they may greatly affect analysis and predictions, structural fractures must be identified. One statistical tool for checking whether a model parameter deviates considerably from a predicted value is the Wald test. To determine whether the coefficients before and after a structural break in a time series model are substantially different from each other, the Wald test may be used. Wald test statistic formula is

$$W = [(\theta\_hat - \theta\_0) / SE(\theta\_hat)]^2$$

where θ_hat is the estimated value of the parameter, θ_0 is the hypothesized value of the parameter, and SE(θ_hat) is the standard error of the estimated parameter. Assuming there is no structural break, the test statistic follows a one-degree-of-freedom chi-squared distribution. The null hypothesis is rejected and a structural break is discovered if the computed value of W is larger than the critical value of the chi-squared distribution. According to Table 2, (Table 3)

Table 2. Trends of Cyber Crime in India

Regress India Year						
Source	SS	df	MS	Number of Observation	20	
Model	4.2446e+09	1	4.2446e+09	F(1,18)	43.11	
Residual	1.7721e+09	18	98452450.1	Prob>F	0.0000	
Total	6.167_09	19	316668859	R-squared	0.7055	
				AdjR-squared	0.6891	
				RootMSE	9922.3	
India	Coefficient	Std.err.	t	P>|t|	[95%conf.interval]	
	2526.421	384.7711	6.57	0.000	1718.047	3334.795
Year-conc	-5069808	773970.2	-655	0.000	-6695859	-3443757

Table 3. No structural break in India

Test	Statistic	p-value
Supremumwald	207.5475	0.000

The Pattern of Financial Cybercrime in India

Here we will discuss the common trends in cybercrime targeting India's financial sector. The trend of financial cybercrime may be discovered by analysing certain forms of financial cybercrime. In both countries, virus attacks, identity theft, online banking frauds, lottery frauds, and so on are among the top five financial cybercrimes. Here are the statistics on cybercrime in the banking sector: (Table 4) (Figure 3).

Table 4. The Pattern of Financial Cybercrime in India

	Ransomware attacks	Identity theft	Credit & debit fraud	ATM Frauds	Online banking frauds	OTP frauds
2021	648	4071	1624	1899	4823	2028
2020	727	5148	1194	2160	4047	1093
2019	1023	12255	367	2067	2093	549
2018	1218	6688	309	1284	968	319
2017	300	3724	395	1543	804	334
Slope	**20.5**	**-84.6**	**334.3**	**158.8**	**1111.7**	**416.2**

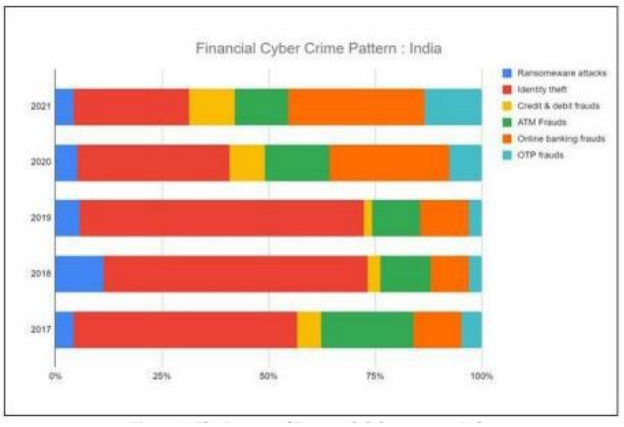

Figure 3. The Pattern of Financial Cybercrime in India

Economic Impact of Cybercrime in India

1. Financial Losses and Damages:

Businesses, people, and the Indian economy are all hit hard by cybercrime, which results in substantial financial losses. The following are some of the monetary effects of cybercrime in India:

a. **Direct Financial Losses:** When cybercriminals commit fraud, steal money, or gain unauthorised access to bank accounts, victims suffer direct financial losses. Theft of money causes huge monetary losses, which individuals and companies have to deal with.

b. **Indirect Financial Losses:** Reputational harm, distrust from customers, and diminished fait from investors are all examples of indirect finncial losses that may result from cybercrime occurrences. Company operations, client acquisition, and economic development as a whole are all susceptible to these variables.

c. **Legal and Regulatory Expenses:** Cybercrime often causes organisations to shell out cash for investigations, litigation, and meeting regulatory requirements. These expenses increase the financial strain even further.

2. Business Disruption and Productivity Losses:

Cybercrime disrupts business operations and causes productivity losses, impacting the overall economic performance. The consequences include:

a. Service Disruption and Downtime: Websites, online services, and vital infrastructure may all become unreachable due to cyberattacks like distributed denial-of-service (DDoS) assaults. Profits go out the window, customers aren't happy, and output drops.

b. Delays in Operational Processes: Businesses hit by cyber attacks may see a holdup in their usual activities like manufacturing, managing their supply chain, or delivering services. Economic inefficiencies result from this disruption of the movement of goods and services.

c. Expenses Associated with Business Continuity: Companies spend money on cybersecurity measures, backup systems, and disaster recovery plans in reaction to cyber threats. The total economic effect of cybercrime is augmented by these further expenses.

3. Intellectual Property Theft and Economic Espionage:

Cybercriminals often target valuable intellectual property (IP) and engage in economic espionage, causing significant damage to innovation and economic competitiveness. The impact includes:

a. **Intellectual Property Theft:** Trade secrets, research results, and other sensitive information are stolen by cybercriminals via cyber espionage, which causes firms to suffer economic losses. This impedes technical progress and reduces the competitive edge.

b. **Piracy and Counterfeit Goods:** Software, entertainment, and pharmaceutical sectors lose money due to the sale and distribution of pirated digital content and counterfeit items made possible by online platforms.

c. **Industry-Specific Economic Impacts:** Intellectual property theft and economic espionage impede the development, investment, and job prospects of targeted sectors. The most vulnerable sectors to cybercrime are those dealing with technology, R&D, and the creative industries.

4. Increased Costs of Cybersecurity:

The rising threat of cybercrime necessitates increased investments in cybersecurity measures, imposing additional costs on businesses and the economy. These costs include:

a. **Cybersecurity Foundation:** Firewalls, IDS/IPS, encryption, and security software should all be part of a company's solid cybersecurity foundation. Operating expenses rise as a result of these investments.

b. **Staff and Expertise:** It takes a lot of money to build a cybersecurity staff that is knowledgeable and to hire outside expertise to fight cyber attacks. It becomes more expensive when cybersecurity experts are hired and when staff are trained.

c. **Compliance and Regulation:** Organisations incur compliance expenses due to the fact that regulatory mandates and industry standards necessitate the adoption of cybersecurity best practices. Infractions might lead to fines or harm to one's reputation.

Cybercrime has a significant economic impact on India, highlighting the critical need for strong cybersecurity measures and more investments in resilience. Resolving these issues may improve economic development, safeguard intellectual property, reduce financial losses, and strengthen economic and social security in India.

Crime Prevention Model for Financial Cybercrime

The crime prevention model takes a holistic approach to preventing cybercrimes by addressing their many facets. Cybercrime prevention measures have been discussed in several conferences and conventions, such as the Budapest convention, among others. In order to provide a novel and workable strategy for preventing cybercrime, this model has taken cues from both national and international agreements. This methodology is primarily composed of five parts: psychological, organisational, capacity building, legal, and technical. (figure 4).

Because cybercrime affects countries all around the world, finding effective solutions will need international cooperation. When it comes to decreasing cybercrime and reacting proactively to incidents, the world's authorities should take the lead in developing the necessary framework. With these five components in place, cybercrime may be mitigated to some extent. There are many ways to look at each of these components in order to avoid offences. Legislative safeguards are necessary to prevent such atrocities. The global character of the crime necessitates concerted international effort to define and criminalise each offence. It is imperative that all statutes and regulations have the resources necessary to protect the public.

Figure 4. Crime Prevention Model for Financial Cybercrime.

CONCLUSION

In conclusion, there is an immediate need for thorough cybersecurity measures and strong countermeasures, according to a research on financial cybercrimes that includes their patterns, trends, and economic effect. Governments, companies, and people are all vulnerable to financial cybercrimes, which have far-reaching effects on the

economy. The ever-changing strategies used by cybercriminals to attack people, institutions, and financial systems may be better understood via research on financial cybercrimes. The best way for lawmakers, cybersecurity experts, and law enforcement to combat these threats is for everyone to have a firm grasp of the patterns and trends already visible. Encourage research and development efforts: Promoting cybersecurity, data protection, and new technology research and development may help us remain one step ahead of cyber threats and encourage innovation in this sector. Cybercrime has far-reaching consequences for the Indian economy, which need investigation into its impact on FDI, industrial competitiveness, and GDP development. The best way for lawmakers, cybersecurity experts, and law enforcement to combat these threats is for everyone to have a firm grasp of the patterns and trends already visible. The economy is greatly affected by financial cybercrimes. People who fall for scams and companies and banks who are the targets of sophisticated assaults both lose a lot of money.

REFERENCES

1. Khan, N.F., Ikram, N. & Saleem, S. (2023), Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Secur J* . https://doi.org/10.1057/s41284-023-00375-4

2. Gourav Singh (2023), Cybercrime in India: Trend, challenges and mitigation strategies, International Journal of Law, Policy and Social Review, Volume 5, Issue 3, 2023, Page No. 95-99

3. Kshetri, Nir (2016). "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future" Crime, Law and Social Change, 66 (3), 313–338.

4. Chen S, Hao M, Ding F, Jiang D, Dong J, Zhang S, Guo Q, Gao C. Exploring the global geography of cybercrime and its driving forces. Humanit Soc Sci Commun. 2023;10(1):71. doi: 10.1057/s41599-023-01560-x. Epub 2023 Feb 23. PMID: 36852135; PMCID: PMC9947441.

5. Ho, H.T.N., Luong, H.T. (2022), Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. SN Soc Sci 2, 4. https://doi.org/10.1007/s43545-021-00305-4

6. Kshetri, N. (2015). India's cybersecurity landscape: the roles of the private sector and publicprivate partnership. IEEE Security and Privacy, 13(3), 16–23.

7. Bures, O. (2013). Public-private partnerships in the fight against terrorism? Crime Law and Social Change, 60(4), 429–455.

8. Salifu, A. (2018). Can corruption and economic crime be controlled in developing economies - and if so, is the cost worth it? Journal of Money Laundering Control, 11(3), 273–283.

9. Dilek S, Çakır H, Aydın M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. Int J Artif Intell App. 2015; 6(1), 21–39.

10. Jaishankar K. The Future of Cyber Criminology: Challenges and Opportunities1. Int J Cyber Criminol. 2020;4(1/2):26.

11. Rid T, Buchanan B. Attributing cyber attacks. J Strateg Stud. 2015;38(1-2):4-37.

12. Broadhurst R. Developments in the global law enforcement of cybercrime. Policing: Int j police sci manag. 2016;29(3):408-33.

13. India emerging as major cyber crime centre (2019), Available at: http://wegathernews.com/ 203/indiaemerging-as-major-cyber-crime-centre/, Visited: 10/31/09

14. Hemraj saini,Yerra Shankar Rao,T.C.Panda — Cyber crime and their Imapct A Review‖ IJERA March 2012 ,Vol 2 P.P No 201-206

15. Kshetri, N. (2013). Cybercrimes in the former Soviet Union and Central and Eastern Europe: current status and key drivers. Crime Law and Social Change, 60(1), 39–65.

Corresponding Author

S. Nakkeeran*

Research Scholar, University of Technology, Jaipur, Rajasthan, India

Email: advocatekeeran@gmail.com