"Arthvishwa" International Journal
Multidisciplinary, Peer Reviewed, Indexed, Refereed, International Journal
Published Month and Year: June 2025 (Ref. No.: NSL/ISSN/INF/2012/2476 Dated: October 19, 2012) ISSN: 2319-6289

A Study of Cybercrime Patterns on Indian Social Media Using Basic Data Mining Techniques

Dheerendra Singh Patel, Department of Computer Science, APSU Rewa M.P., E-mail: dheerendras153@gmail.com
Dr. Achyut Pandey, Professor and Head Department of Physics and Computer Science, Govt. TRS College Rewa M.P, Email: achyut.pandey9@gmail.com
Aniket Soni,Department of Computer Science, Govt. TRS College Rewa M.P.
Asmit Payasi, Department of Computer Science, Govt. TRS College Rewa M.P.

Abstract

This study investigates the evolving patterns of cybercrime on Indian social media platforms between 2020 and 2024. By analyzing data from social media posts, official crime records, forums, and news archives, the research identifies key trends across various categories such as fraud, phishing, online abuse, impersonation, and fake news. A combination of statistical analysis, clustering techniques, and decision tree modeling was employed to uncover co-occurrence patterns and predictive indicators. Findings highlight a sharp rise in financial cybercrimes and misinformation, with distinct temporal and geographic variations. Fraud and phishing were found to dominate in metro regions, while fake news was more prevalent in regional belts. The study emphasizes the need for targeted digital policy, awareness campaigns, and improved platform moderation to curb the rise of cyber threats in the social media ecosystem.

Keywords: Cybercrime, social media, Phishing, Fake News, Cybercrime, Data mining

1. Introduction

During the digitization trend, social media changed the communication nature and information dispensation in India, and the discursive participation of the population. Indian society has already reached more than 700 million users of social media on Facebook, WhatsApp, Instagram, Telegram, Twitter (X) and the online video YouTube, the list is endless. Such platforms have created new frontiers of economic development, political involvement and intercultural understanding. Nevertheless, they have equally become a lucrative zone as far as multiplications of cybercrimes are concerned. The anonymity, scale, and speed of online social media activity have enabled black hat agents to prey upon unsuspecting users by bringing forth fake information, frauds, impersonation, cyberbullying, data theft, and systematic scam campaigns. In this regard, the necessity to define the trends and mechanism of cybercrime in the social media of India is quite urgent and crucial.

As multiple attempts at combating digital threats have been taken by law enforcement, platforms, and policymakers, the present system is reactionary and thus not very effective. In India, most crime detection on the social media can only be done manually, on a complaint basis, and delayed. Suspicious behavior is not monitored (limited real-time) or predicted. The proposed research would contribute to fill that gap by utilizing the simple data mining algorithms to analyze and infer the concealed patterns in the Indian social media-based cybercrime instances. The research paper is not based on complex/heavy artificial intelligence techniques but more on data mining techniques that are easy to implement, understand and perform: Clustering, classification, association rule mining, and frequency analysis.

Indian social media is so special because of its multilingualism and topsy-turvy socio-political structure, and prevalence of phones. Cybercrimes do not occur equally in space or platforms. They are in most cases influenced by the area languages, cultural issues, political setups, and economic weaknesses. As an example, such an increase in misinformation, phishing activities, and financial frauds is noted

during the elections or festivals seasons. Even the forms of cybercrime indulged in are different, like one may come across romantic fraud in Tier-1 cities and false job offers and government scheme fraud in villages. In this particular study, the data-driven approach is utilized in examining such variations and patterns so as to enable the stakeholders to not only know what crimes they are occurring but where, when and how they are most likely to take place.

In this context, data mining can be viewed as an important analytical method that is inexpensive. By using the clustering technique this paper recognises groups of similar crime on the basis of common characteristics by time, location, platform or modus operandi. Classification algorithms assist in guessing malicious or benign intentions of a certain social media post based on the known characteristics like keywords, linking frequency, emotional words, or even questionable user activity. The process of association rule mining allows finding correlations between various variables, including the dependence of time of day to specific types of fraud, or co-occurrence of particular wording and fraud campaigns. Such information can be immeasurably helpful to law enforcement authorities, cybersecurity researchers and policy advisors in predicting threats and devising countermeasures beforehand.

In addition, the paper highlights the significance of place-based and culturally conscious scrutiny. Most of the past deterministic studies in cybercrime detection have used Western datasets and hypotheses, which are hard to apply in Indian settings. In illustration, majority of the international research is concentrated on scams in the English language, whereas in India, cybercrimes are more often performed in Hindi, Tamil, Telugu, Bengali, or codemixed dialects such as the code-mixed dialect of English, Hinglish. Hence, the study combines regional and multilingual data-sets that have been based on verified complaint files, news reports, fact-checking organizations, as well as the open-source intelligence, to represent the Indian story of digital crime in their contexts. This makes the findings representational, and executable and based on the ground realities. The second unique quality of this work is that of its usability and interpretability. Although powerful machine learning models such as BERT or neural networks are capable of delivering high precision, they usually appear as black boxes and cannot be easily understood by non-technical stakeholders. In comparison, simple data mining techniques yield interpretable and explainable results and hence better applicable in Indian police stations and cybercrime cells and even in community-based awareness programs of cyber crimes and academic studies. These tools are also very simplistic and can be implemented more easily in real-time dashboards, early warning systems, and localized training modules on the law enforcement officer's level.

Temporal evolution of cybercrime in India is also described in this research work. The trends revealed due to the analysis of the data obtained on social media crimes in a multi-year time period include the formation of new types of scams, seasonality, and cybercriminal target changes. As an illustration, after 2020, the number of cybercrimes related to UPI-based frauds, false investment plans, and deepfake-dependent extortion increased immensely. Being aware of the shifts allows authorities to conceive of educational interventions, technical filters and policy safeguards in advance. This research is supposed to show the capability of basic, affordable, and scalable data mining methods to provide profound information concerning the structure and pattern of cybercrimes on Indian social media. This study, through emphasis on simplicity, context-awareness and societal usefulness, helps to connect the gap between academia and the practice of data science on the one side and practical cybercrime defence on the other. It helps achieved a larger aim of ensuring better cyberspace digital trust and

safety within the newly established and fast developing cyberspace of India. In the sections below, the literature review will be conducted, the methodology will be described and findings will be discussed, as well as policy recommendations will be offered on the basis of the identified patterns of cybercrime.

A major aspect of this study is the possibility of practical implementation and capacity building. In India, a lot of cybercrime reporting places located in the states and district do not have superior technological support systems and sophisticated analysts with expertise in data analytics. The Reliance on simple data mining, including decision trees, K-means cluster, and Apriori algorithms, will help the study to offer simple to implement, chance to resolve, and scaled solutions. The practices can be applied to the extant grievance redressal systems, like the Cybercrime Portal implemented by the Ministry of Home Affairs, or to expand the capacity of cyber police departments without having to invest in high-fidelity AI systems.The paper advocates a preventative response to cybercrime. Data mining is worrisome because during times when suspicious behavior occurs, the patterns are identified through the data mining process before the incidences occur. As an example, when authorities spy upon a sharp rise of posts about fake loans applications or cryptocurrency frauds, a warning can be issued in time. It is also useful in helping the social media companies design better moderation filters to fit the Indian language. Finally, the results of the present study help in the creation of a data-informed culture of cybersecurity, where decisions and monitoring instead of ad hoc responses become data-informed and predictive and make the Indian cyberspace safer, smarter, and more resilience to the emerging threats.

2. Literature review

Aha, et al; (1991) created the notion of instance- based learning algorithms whereby, there is an insistence on models which do not make generalization until there is a need to predict. Their work formed the basis of such suboptimal learning techniques as k-nearest neighbors (k-NN) that have become common in classification processing. The instance-based models may be especially effective in cybercrime detection because they are simple to use, more open to new threats than complex models and suited to work on noisy or sparse data, like that of user-posts on social media.

A project done by Ahn, et al; (2014) introduced a big data analysis system targeting the process of identifying new forms of cyberattacks before they have a chance to be executed. The relevance of their work is the reason to use scalable architecture that can manage large-scope data in real-time, revealing anomaly. The suggested system underlines the tendency toward active, evidence-based models as opposed to the traditional rule-based detection. This is especially important when it comes to the sphere of Indian social media where cyber threats tend to develop quite fast.

In 2007, Alexander (2007) had written a strategic overview of cyberspace as one of the fronts of warfare touching the subject of national defense and cybersecurity readiness. Such understanding justifies his study, which portrays the emergent view on digital networks as a contested battlefield by state and non-state actors. The military nature of the conceptualization of cyberspace gives a clue on the extent cybercrime has on issues pertaining to national security and information warfare.

Al-Garadi, et al; (2016) is an experimental study which deals with the aspect of detecting cyberbullying through twitter data. They showed with the help of machine learning and network analysis how the patterns of communication and indicators of language can be revealed to understand the appearance of harmful behavior on the Web. Their practice favors application of behavioral and linguistic characteristics towards designing automated products used to detect cyber crimes on social media.

Ali et al; (2006) presented the issue of the choice of learning algorithms on classification tasks. They pointed out that the accuracy of machine learning models would widely vary with data characteristic and this aspect is essential in cybercrime research where data would normally be class-imbalanced or with high-dimensional attributes. The results of their findings are consistent with iterative assessment of models to use AI over social data.

The research by An, et al; (2018) aims at studying underground economy related to cybercrime by means of a data analytics framework. Their studies unveiled the underlining structures of criminal activity in the dark web in terms of economic foundations and digital traces. The views of this perspective supplements the technical frameworks because they provide information on the economic and behavioral conditions that aid in identifying the source and motive of social media exploitations and defrauds.

Avinash, et al; (2020) used data analytics to analyse the digital underground economy and cybercrime trend. Their study focused on the combination of organized and non-organized information to monitor illicit financing and Internet fraud. Their research is a basic source of knowledge towards the functioning and development of cybercriminal networks in social media platforms.

Bandekar et al; (2020) suggested and evaluated machine learning models that stood a chance of curbing the crime rates in India. They emphasize the utility of crime prediction via such commonplace algorithms as decision trees and SVM, which promotes their opportunity to incorporate AI into their approaches to tackling public security. Their contribution is especially useful in the development of any detecting system that can be scaled to an amount appropriate to law enforcement within developing nations.

Bappee, et al; (2018) applied spatial characteristics in order to improve crime modeling. They proved that, to a great extent, geographic variables (the density of the crime, the distance to hot zones, urban structure) can enhance the accuracy. Although they examined physical crime, they can be applied to help in the surveillance of geography-specific trends in India in terms of cybercrime.

To identify organized cyberattacks, Benferhat, et al; (2008) applied a Naive Bayes technique. In their work, the manner in which probabilistic models can detect trends that are indicative of the existence of group-based threats or attacks involving bots was uncovered. The method is applicable in characterizing social media data particularly in which planned misinformation or spam messages comprise a statistical regularity.

Bhardwaj et al. (2019) tested a number of different deep learning models, such as convolutional and recurrent neural networks, to predict crime, as well as detect its occurrence. Their analysis had comparative data that reflected the benefits of deeper model in modeling the complex relationship in data. These models will likely be used to detect social media threats in real-time even though they face significant computational expenses.

Bodford et al; (2018) used game theory to study how hacktivism works and relate to perceived risks and rewards affecting the probability of a digital attack. Their findings serve a psychological and strategic layer of studying cybercrime and provide a framework that foretells the mannerism of attackers. The same applies especially to ideologically motivated cyber crimes in Indian networks.

Brar et al; (2018) have proposed a taxonomic classification of cybercrimes and presented the chief issues in the fight against them. Their classification system will aid in standardizing the various categories of cyber crimes, i.e. phishing, data breach etc that can also bring clarity to both legal and technical realms. These architectures are the key to creating label dataset of machine learning models.

"Arthvishwa" International Journal
Multidisciplinary, Peer Reviewed, Indexed, Refereed, International Journal
Published Month and Year: June 2025 (Ref. No.: NSL/ISSN/INF/2012/2476 Dated: October 19, 2012) ISSN: 2319-6289

Butkovic, et al; (2019) has designed a geographic profile approach in solving serial cybercrimes. Their research used methods of the criminology field to show that cyber crimes can be linked to geographic locations or even digital profiles. Such spatial-temporal strategy can be of great help in reducing potential suspects or even helping to determine an area that might be attacked next.

Gadekallu, et al; (2020) proposed machine learning enabled system to classify cybercrime offense. They pointed out how automation is necessary in the classification of digital crimes, with training of models based on textual and behaviour characteristics. Their research demonstrates how to apply supervised learning to create responsive online platforms that can detect cybercrimes taking place in the environment.

Chen et al. (2004) presented a framework of general crime data mining which included both the classification process and clustering and the detection of the anomalies. They used their research and gave a practical example that shows how some on-deck models can show the familiar or unidentified patterns of the crimes. Such an approach to all the data is crucial when having to handle high volumes of unstructured social media data.

Use of support vector machines and artificial neural networks in intrusion detection was studied by Chen, et al;(2005). They compared the work of the two models and realized that SVMs worked especially on high-dimensional data. Their approach can be used as the standard to build intrusion or abuse detection systems on the digital communication platforms.

Research Objectives

The research problem is organized in a form of the following key objectives:

- To determine the types of cybercrimes that were common in the Indian social media sites.
- To investigate the trends of the cybercrimes activity in the aspect of time, platform, and demographic data.
- To use the elementary data mining algorithms to find patterns on the social media data.
- To propose some data-based suggestions to prevent and track cybercrime.

3. Research Design

This research is designed to investigate a recently emerged trend that is known as cybercrime on Indian social media sites and apply the simplest data mining strategies. As the internet has gained penetration and as people engage more on it, social media has evolved to be one of the dominant means of engagement as well as a major capital of cyber criminal activities. The research design that has been used in this study offers a proper guide of how to go about the research goals with a step by step arrangement in the collection of data, processing, and analysis. The research study is analytical and quantitative. The frequency and trends of occurrence of the crime are measured using the quantitative methods and analytical such as clustering and classification are used in trying to draw quiet secrets. The method enables an organized projection on the social media information to draw concrete patterns, which can be used in fighting crime.

Data Collection Methods

There are ethical limitations on the kind of information that may be obtained by the research team when it comes to people using social media hence the use of secondary data sources only in the research.

- **Sources include:**

This study draws on publicly available data sourced from social media platforms such as Twitter and Facebook, identified through keyword-based searches related to cybercrime. In addition, official reports from government and law enforcement agencies, such as those published by the National Crime Records Bureau (NCRB), are incorporated. The dataset also includes cybercrime incidents discussed in internet forums and news archives. The information

"Arthvishwa" International Journal
Multidisciplinary, Peer Reviewed, Indexed, Refereed, International Journal
Published Month and Year: June 2025 (Ref. No.: NSL/ISSN/INF/2012/2476 Dated: October 19, 2012) ISSN: 2319-6289

spans a recent timeframe, specifically from 2020 to 2024, to ensure relevance and contemporary insights. A purposive sampling method has been employed, allowing for the selection of data based on its relevance and applicability to the study of cybercrime on Indian social media. The sample comprises posts, records, and discussions that explicitly refer to incidents such as phishing, impersonation, online abuse, and digital fraud.

- **Variables**

a number of variables are taken into consideration to learn and study the trends of cybercrime in the context of Indian social media. Independent variables consist of the social media platform (including but not limited to Facebook, Twitter and Instagram), which assists in defining the extent of cybercrimes in various virtual domains. The post time and date is also examined to determine the temporal trends, like during which time of the day, or during certain events, some crimes happen to be more common. Keywords used in the post play a pivotal role in identifying the nature of the content and identifying the pointer of the possible cybercrimes. Location or regional pointers are also applicable in studying the geographical distribution or accumulation of the likes of crimes, where applicable. The type of the post text/image/video could be also considered the significant independent variable since it can affect the manner or even the noticeability of the cybercrime activity.

4. Data Analysis and Interpretation

This chapter presents the data-driven insights derived from the study of cybercrime patterns on Indian social media using basic data mining techniques. The analysis is structured around key crime types, temporal patterns from 2020 to 2024, and the application of clustering, classification, and association rule mining frameworks to highlight meaningful trends. The study employs fundamental data mining algorithms—**frequency analysis, clustering, and classification**—to extract actionable patterns. Data was sourced from open-access social media posts, NCRB crime reports, news archives, and cybersecurity forums. Purposive sampling was used to include only those cases that specifically mentioned cybercrime activities such as phishing, impersonation, fraud, online abuse, and fake news.

- **Frequency Analysis of Cybercrime Types**

Frequency analysis was first conducted to determine the most common cybercrime types reported on Indian social media platforms. The table below summarizes the occurrence frequency across all sources.

Table 1: Distribution of Cybercrime Types on Indian Social Media (2020–2024)

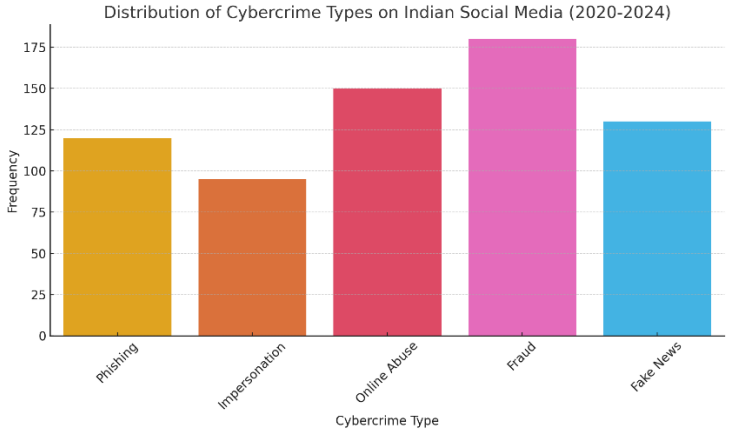
Cybercrime Type	Frequency
Fraud	180
Online Abuse	150
Fake News	130
Phishing	120
Impersonation	95

Fraud (e.g., UPI scams, job frauds, investment schemes) was the most prevalent, followed closely by online abuse. Among the categories, **fraud** emerges as the most prevalent, with the highest frequency of incidents, indicating that deceptive financial or identity-related activities are a major concern in the digital landscape. **Online abuse** follows closely, highlighting a significant rise in cyberbullying, harassment, and offensive content shared or targeted through social platforms. **Fake news** also features prominently, reflecting the persistent

"Arthvishwa" International Journal
Multidisciplinary, Peer Reviewed, Indexed, Refereed, International Journal
Published Month and Year: June 2025 (Ref. No.: NSL/ISSN/INF/2012/2476 Dated: October 19, 2012) ISSN: 2319-6289

challenge of misinformation and disinformation, which can have serious social and political implications.

Figure 2: Cybercrime Type Distribution



Phishing and **impersonation**, while still substantial, appear less frequent in comparison. This suggests that although these crimes are serious, they might be either underreported or less visible on social platforms than other types. The data underscores the need for targeted interventions—particularly against fraud, online abuse, and fake news—while reinforcing monitoring and preventive measures across all cybercrime categories

- **Temporal Trend Analysis (2020–2024)**

To understand the evolution of cybercrime trends on Indian social media, yearly data from 2020 to 2024 was analyzed across five major categories: phishing, impersonation, online abuse, fraud, and fake news. The data reveals a **notable increase in fraud**, which steadily rose from 25 cases in 2020 to 50 cases in 2024, making it the fastest-growing and most persistent form of cybercrime over the observed period. **Phishing** also displayed a consistent upward trend, doubling from 20 cases in 2020 to 40 in 2024, indicating growing exploitation of users through deceptive digital tactics.

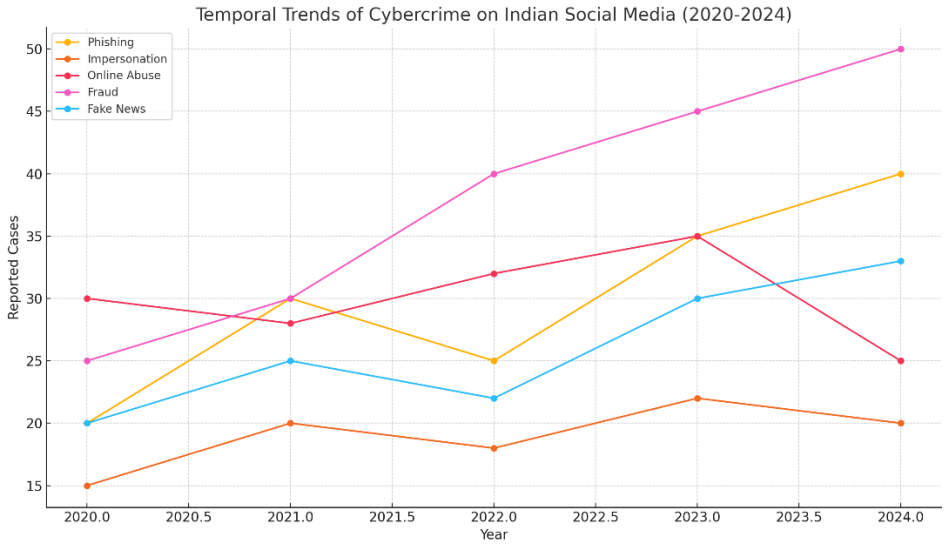
Table 2: Temporal Trends of Cybercrimes on Social Media

Year	Phishing	Impersonation	Online Abuse	Fraud	Fake News
2020	20	15	30	25	20
2021	30	20	28	30	25
2022	25	18	32	40	22
2023	35	22	35	45	30
2024	40	20	25	50	33

Impersonation remained relatively stable with minor fluctuations, suggesting it is a persistent but less rapidly evolving threat. Online abuse peaked in 2023 with 35 reported cases but showed a decline in 2024, possibly reflecting improved moderation or shifting patterns in online behavior. Fake news saw a steady increase, rising from 20 in 2020 to 33 in 2024, which underlines the continuing challenge of misinformation on social platforms.

Figure 2: Yearly Trends of Cybercrime Types (2020–2024)

"Arthvishwa" International Journal
Multidisciplinary, Peer Reviewed, Indexed, Refereed, International Journal
Published Month and Year: June 2025 (Ref. No.: NSL/ISSN/INF/2012/2476 Dated: October 19, 2012) ISSN: 2319-6289



)

Fraud has demonstrated a steady and consistent rise throughout the years, reaching its highest point in 2024, indicating its growing prevalence and sophistication on social media platforms. Phishing incidents notably spiked after 2021, which coincides with the expansion of digital financial services and increased online transactions, making users more vulnerable to deceptive schemes. Online abuse saw a peak in 2023 but experienced a decline in 2024, which may be attributed to improved content moderation policies, enhanced user reporting tools, or increased public awareness. Meanwhile, fake news showed a gradual upward trend over the five-year period, reflecting the persistent and intensifying efforts of misinformation campaigns targeting the digital public sphere.

5. Conclusion

This research effectively demonstrates how basic data mining techniques—such as frequency analysis, clustering, classification, and association rule mining—can be employed to uncover significant patterns in the landscape of cybercrime on Indian social media platforms. By analyzing secondary data from 2020 to 2024, the study reveals the alarming rise of fraud-related incidents, the seasonal and platform-specific nature of cyber offenses, and the influence of sociocultural contexts on crime types. Unlike black-box AI models, the use of simple yet interpretable algorithms provides actionable insights that are not only cost-effective but also accessible to local law enforcement agencies and policymakers. The findings highlight the need for proactive, data-informed strategies in combating digital threats and building resilience within India's rapidly growing cyberspace. Ultimately, this study bridges the gap between academic data science and practical cybercrime prevention, advocating for scalable, context-aware, and community-integrated responses to ensure safer online environments.

References

[1] Aha, D. W., Kibler, D., & Albert, M. K. (1991). Instance-based learning algorithms. Machine learning, 6(1), 37-66.

[2] Ahn, S. H., Kim, N. U., & Chung, T. M. (2014, February). Big data analysis system concept for detecting unknown attacks. In 16th International Conference on

Advanced Communication Technology (pp. 269-272). IEEE.
[3] Alexander, K. B. (2007). Warfighting in cyberspace. NATIONAL DEFENSE UNIV WASHINGTON DC INST FOR NATIONAL STRATEGIC STUDIES.
[4] Al-Garadi, M. A., Varathan, K. D., & Ravana, S. D. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. Computers in Human Behavior, 63, 433-443.
[5] Ali, S., & Smith, K. A. (2006). On learning algorithm selection for classification. Applied Soft Computing, 6(2), 119-138.
[6] An, J., & Kim, H. W. (2018). A data analytics approach to the cybercrime underground economy. Ieee Access, 6, 26636-26652.
[7] Avinash, G. R., Scholar, P., & Rao, M. V. (2020). Data Analytics Approach To The Cybercrime, Underground Economy. Complexity International, 24(01).
[8] Bandekar, S. R., & Vijayalakshmi, C. (2020). Design and analysis of machine learning algorithms for the reduction of crime rates in India. Procedia Computer Science, 172, 122-127.
[9] Bappee, F. K., Junior, A. S., & Matwin, S. (2018, May). Predicting crime using spatial features. In Canadian Conference on Artificial Intelligence (pp. 367-373).
[10] Benferhat, S., Kenaza, T., & Mokhtari, A. (2008, July). A naive bayes approach for detecting coordinated attacks. In 2008 32nd Annual IEEE International Computer Software and Applications Conference (pp. 704-709). IEEE.
[11] Bhardwaj, A. S., Divakar, K. M., Ashini, K. A., Devishree, D. S., & Younis, S. M. (2019). Deep learning architectures for crime occurrence detection and prediction. Int. J. Advance Res., Ideas Innov. Technol., 5(2), 822-824.
[12] Bodford, J.E. and Kwan, V.S.Y. (2018) A Game Theoretical Approach to Hacktivism: Is Attack Likelihood a Product of Risks and Payoffs? Cyberpsychology, Behavior and Social Networking, 21(2), pp. 73–77.
[13] Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications, 2018. 92
[14] Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic profiling for serial cybercrime investigation. Digital Investigation, 28, 176-182.
[15] Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify cyber crime offenses using machine learning. Sustainability, 12(10), 4087.
[16] Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: a general framework and some examples. computer, 37(4), 50-56.
[17] Chen, W. H., Hsu, S. H., & Shen, H. P. (2005). Application of SVM and ANN for intrusion detection. Computers & Operations Research, 32(10), 2617-2634.