



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Knowledge-Based System for analyzing Cyber Crimes

Mrs. K. Chitra Lekha^a, Dr. S. Prakasam^b

^aPh.D Research Scholar, Department of Computer Science and Applications, SCSVMV University, Kanchipuram, India

^bAssociate Professor, Department of Computer Science and Applications, SCSVMV University, Kanchipuram, India

ABSTRACT

The Knowledge-Based system should be competent to spot out cyber crime patterns rapidly and in a proficient approach for upcoming recognition of cyber crime prototypes. In the current situation, the subsequent main disputes are encountered: Cyber crimes are tremendously thorny to spot out the scandalous; the digital indications of these scandalous are also effortlessly swabbed by them; moreover the pace of the cyber offenses has amplified at a frightening rate that it has virtually turned out to be unfeasible to thwart a cybercrime from occurring; many times the cyber offence remains unreported as cyber victims are innocent of such offences; investigation of cyber crime requires proficient experts to execute the challengeable tasks; the issues in accumulating and scrutinizing of these increasing amounts of cyber crime data. All the exceeding disputes motivated this study to focus on affording clarifications that can augment the process of cyber crime analysis for recognizing and decreasing cyber crimes in India. Thus the main focus is to develop a Knowledge-Based system that assists the law enforcement and the cyber crime victims in perceiving cyber crime patterns in India and execute investigation of cyber crimes; scrutinizing cyber crime prototypes to shrink occasions of analogous prevalence; generating facts to devise approaches for cyber crime anticipation; affording details about the punishments of cyber crime under IPC sections and IT Act 2000 and the possible preventive measures undertaken by respondent before and after he has been a cyber victim.

Keywords: Knowledge-Based System, Cyber crime, Prediction, Information Technology

1. Introduction

A Knowledge-Based System (KBS) can be represented as an interactive, computer-based technique intended to signify and motivate with acquaintance of some expert topic with a vision to crack issues and/or generate recommendation utilizing an amalgamation of rules, investigative procedures and information reclamation and these methods facilitate in enhancing and assessing suitable option and overtake a conclusion based on the preeminent choice. It can be very significant in confining, reclaiming and preserving the proficiency in the institution in addition to expediting and enhancing the eminence of services afforded. The intention of Knowledge management systems is to maintain conception, convey and relevance of information in institutions (Alavi et al. 2001). With the accessibility of sophisticated computing amenities and further possessions, concentration would currently spiral to more and more challenging errands, which may involve intelligence. The business and culture were fetching knowledge oriented and rely on diverse experts' decision-making capability. Knowledge-Based Systems can perform as a specialist on stipulate exclusive of wasting occasion, everywhere and at anytime. They could accumulate currency by leveraging specialist, permitting clients to execute at privileged level by supporting reliability. One may believe the KBS as prolific tool, embedding knowledge of more than one specialist for extensive phase of time. In reality, a KBS would be a computer based system, which utilizes and spawn information from facts, information and knowledge.

The Knowledge-Based Systems are competent of perceptive the information under progression and could take assessment based on the dwelling knowledge accumulated in the system while the conventional computer systems do not recognize or identify with the facts/information they execute. The skill of the intelligent systems to confine and reallocate proficiency has momentous inference on progress of a nation or population. Such smart systems permit documentation of one or more specialist acquaintance and exploit the information for problem cracking in cost efficient approach; the import of knowledge in diverse domains that the country lacks; the export of acquaintance concerning to domestic domains of knowledge, and the replication and redeployment of sparse facts in a cost efficient mode (Darek et al. 1991).

1.1 Advantages of Knowledge-Based Systems

Knowledge-Based Systems were more valuable in several circumstances than the conventional information systems that would embrace:

- During non –availability of experts.
- When knowledge from specialists has to be hoarded for prospect exploit or while knowledge has to be replicated or proliferated.
- When intellectual support or guidance were essential for the assessment crafting for the purpose of solving issues.
- When more than one specialist information has to be clustered at a solitary proposal.

With the appropriate deployment of information, the Knowledge-Based Systems enhance production, document odd data by confining scarce proficiency and augment trouble solving competence in a most flexible manner. Such systems also accumulate acquaintance for potential exploit and guidance that would lead to enhancement in quality along with the process of solving issues. Conversely, the paucity and temperament of information would craft the KBS development method thorny and intricate. The translucent and conceptual nature of information has been liable for this and also this domain requires further strategies for the acceleration of the progress method.

Knowledge-Based Systems afford numerous advantages over Natural Intelligent systems that would embrace of the following:

- Knowledge-Based Systems afford proficient credentials of the significant information in a tenable and consistent mode.
- Knowledge-Based Systems crack unstructured, huge and intricate issues in a rapid and intellectual method and afford validation for the assessment recommended.
- Knowledge-Based Systems propose more than one specialist acquaintance in an incorporated approach.
- Knowledge-Based Systems are capable to deduce innovative knowledge and learn from cases or facts instead of just referring the accumulated content.
- It has been simple to make a replica and widen acquaintance and Knowledge-Based Systems.

A number of KBS relevance areas also release profound idealistic concerns. This would expose a promising area of cram whose prime distress has to discover efficient approach for the purpose of recognizing and pertaining intelligence in tackling issues, forecasting and communication expertise for an extensive variety of realistic tribulations. Distinctive information systems transact with facts whereas Knowledge-Based Systems automate proficiency and contract with acquaintance. Every trade in today's aggressive world has been occupied with ambiguity and hazards. Administrating and gratifying clients with eminence manufactured goods/services have become trifling dispute. In this state, the Knowledge-Based System would be a prudent alternative. Despite of ample merits, the development and utilization of the Knowledge-Based System would be thorny as of the issues connected with them. Scientists, researchers and experts are working on diverse phases of Knowledge-Based System to conquer these precincts and to afford a proficient intellectual system which would be companionable with the innate intellectual system in a prescribed manner.

2. Need for Knowledge-Based System in Cyber crime prevention

The investigation of Cyber crime cases has been a discerning province where there is need of proficient techniques for the prediction and classification for the purpose of analyzing the escalating numbers of offense data. The Cyber crime prophecy methods would be assessed and scrutinized by the efficient tool in felony investigation. The prevalent dispute faced by many Law Enforcement officials was how to competently and precisely scrutinize the escalating volumes of offense data (Malleon et al. 2010). The capability to evaluate huge volume of offense data without utilizing computational support would deposit sprain on human brain because human mechanism has been incompetent of realizing with millions of information (Nasar et al. 1993). The Knowledge-Based System should be able to recognize the Cyber Crime prototypes as rapid as probable and in an effectual mode for prospect offense recognition. By utilizing an extensive variety of Data mining processes such as Multilayer Perceptron, Fuzzy clustering, Recurrent Neural networks or Support vector machine, it has been probable to discover supportive information to assist in offense prophecy issues. This also embraces the ability of the system to scrutinize or assess a huge volume of Cyber crime statistics and information from diverse resources. However, to envisage prospect offense precisely with an enhanced concert has been a difficult task as of the escalating occurrences of Cyber crimes in the present days.

The need for prevention of Cyber crimes from occurring has been crucial for the safety, permanence and progress of the humanity. Law Enforcement bureau has been seeking for the system to target Cybercrime prototypes competently. The intellectual offense data investigation would afford the preeminent understanding of the dynamics of illicit tricks, discerning prototypes of scandalous deeds that would be useful to recognize where, when and why felony can transpire. There has been a need for the progression in the data storage assortment, investigation and algorithm that could handle information and defer high precision. Huge volume of facts associated to all types of offenses has been stored in Police station records which may hoard direct or indirect information connected to the offenses and the requirement of technology that would scrutinize necessary information from this large

content from the chronological offense and scandalous association documentation, the scandalous inquiry panel could extort valuable information so that they can spot the facts associated to the dedicated offense and lessen the prospect felony possibilities (Wang et al. 2013).

Perceiving and recognizing cyber offenses in real-time, predominantly for e-banking, is actually an intricate and vibrant issue concerning many aspects and the uncertainties implicated in the recognition, Knowledge-Based System can be an effectual tool in evaluating and spotting cyber offenses for states across India since it affords a more normal way of dealing with eminence aspects rather than precise ideals. The rapid improvement of technology significantly bangs to human life styles; however it would also spawn issues such as emergence of Cyber felony. Application of artificial agent has been a latest drift for combating Cyber crimes as they afford features such as mobility, prudence, malleability and association. Due to the enhancement in Information Technology (IT), scandalous are utilizing cyberspace to commit various cyber felony. Cyber infrastructures are extremely susceptible to incursions and other intimidations. Physical devices and individual intercession has not been adequate for observing and defending of these infrastructures; hence, there has been a requirement for more refined Cyber defence systems that need to be stretchy, malleable and robust, and able to perceive an extensive assortment of threats and craft intellectual real-time assessments. Several bio-inspired computing techniques of Artificial Intelligence have been progressively playing a significant role in Cyber crime recognition and preclusion (Dilek et al. 2015).

In order to lessen the felony rate, the Law enforcements have to take the defensive measures and so with the intend of safeguarding the humanity from cyber offenses, which facilitates the need of advanced systems and novel approaches for enhancing the cyber crime analytics for defending their population. Precise concurrent felony prophecy facilitate to shrink the offense rate but remains challenging issue for the systematic society as incidences of felony depends on many intricate aspects. The occurrence of Cyber crimes has been escalating at a frightening pace and the number of offenses committed presently had been larger than even been before. The common and repetitive Cyber stalking, Cyber bullying, spamming, phishing etc have made the public to have restless hours of darkness and edgy days. They experience very anxious and defenceless in the occurrence of anti-social and malevolence rudiments. The scandalous have been executing the technological offenses in a well organized approach that leaves no indications of such offenses to Law and Enforcement officials which further becomes a huge hectic to them.

The above issue would be solved by the development of Knowledge-Based System which has been a computational paradigm of Artificial Intelligence, Data mining, statistics and Database systems for the purpose exploring Cyber crime prototypes in huge crime datasets. Apart from knowledge implication concerns, it would involve interestingness metrics, intricacy deliberations, post-processing of revealed crime patterns, prophecy, and online updating. Thus the overall goal of the Knowledge-Based System would be to extort facts from Cyber crime dataset and renovate it in to a reasonable form for the Law and Enforcement officials which would be useful for them in forecasting of such cruel offenses before taking place, so that they could be prevented. The process of handling huge volume of offense data manually that has been committed would make felony prevention stratagem a time consuming and intricate job. The process of perceiving that if a felony fits a convinced, recognized prototype or a novel model has been a repeatedly monotonous effort of felony analysts, detectives or police officers themselves. They physically reallocate through heaps of paperwork and indications to envisage, predict and optimistically thwart offense.

Data Mining would be utilized for renovating this raw statistics into significant and decisive information which would facilitate in crafting a Knowledge-Based System for the judiciary and administration for taking steps towards maintenance of felony in check. Sometimes a felony has been linked with intricacies that would spin around idea and involvement with a meticulous locality and further aspects which crafts the analyst's task somewhat tricky. Furthermore, indications could be slackly coupled while being geospatially sparse, utilizing a more wide inquiry exertion. Utilizing the influence of Data mining methods that would instruct the capability to inspect, prophesy, capture into report, and take action beside scandalous behaviors and prospective defence threats.

2. Literature Review

Ozgul, F. (2013) had focused on the utilization of Knowledge innovation in felony analysis, and also the steps implicated in offense exploration. Initially they had considered crime information origins from which the four kinds of knowledge innovation have been formed that could be applied to the most appropriate kind of offense exploration along with the appropriate methodologies, as every crime investigation focuses on diverse kinds of conclusions and knowledge innovation. They had explored what kind of offense inquiry would be preeminent with appropriate kind of methodology along with knowledge innovation utilizing which kind of information. They had concluded that for CRISP-DM and CIA intellect methodologies, clustering and prophecy techniques were appropriate, but for AMPA and Vander Hulst methodologies, cases concerning perceptive associations and the humanity of others with further data training and explicit assessment have been more acquiescent.

SaiVineeth, K. R. (2016) had proposed a work on exploring recurrent crimes state wise utilizing FP Max a bottom up method that implements linked lists for reduction of space complexity. They had utilized correlation analysis and afforded crime intensity points for all states in India per year. From this, classification had been done utilizing Random Forest to categorize the states as most dangerous, dangerous, moderate and safe crime prone areas.

Pande, V. (2016) had anticipated a system to extort data from crime record repositories, from which they had intended to execute data mining. They had trained a set by utilizing data classification and regression algorithms and then applied these learned rules on the test set in order to decide the envisaged results. This augmented work had extracted massive quantity of raw data by producing it in the form of a crime data set and it had preprocessed them. The diverse data mining algorithms when applied on those crime datasets had fabricated outcomes that would be of enormous prospective exploit to law enforcement agencies particularly.

Bogahawatte, K. (2013) had offered a system of recognizing a scandalous by utilizing existing evidences in circumstances where any witness or forensic traces were not present. Based on the existing facts, it had segmented the crime data in to subsets by utilizing a precise clustering algorithm and it had also utilized Naïve Bayesian classifier to recognize most potential suspect for crime occasions. The system had utilized the communication authority of multi agent systems to augment the efficiency in recognizing probable suspects.

3. Knowledge Based System

The Knowledge-Based System is a system program that utilizes a knowledge base along with inference engine to resolve intricate tribulations. It is effectively self-possessed of two sub-systems: the knowledge foundation and the deduction engine. The knowledge foundation corresponds to information concerning the world. The deduction engine is a mechanized interpretation method that assesses the modern situation of the knowledge-base, concern pertinent conventions, and then emphasizes innovative acquaintance into the knowledge base. The intention of information innovation is to extort valuable knowledge, while the endeavor of offense exploration is to unravel and shed light on mysterious feature of what truly had occurred. The enhancement of systems that craft utilization of facts, perception and intellect are a pace towards confectioning this dispute. The classic expert systems transact with facts while Knowledge-Based systems mechanize proficiency and compact with knowledge.

The registered cyber crime cases in selected states of India were gathered for the period from 2007 to 2018 and stored in the cyber crime database. The IT Act and IPC sections of diverse cyber crimes along with the punishment and penalty for the same have also been gathered and were stored in cyber crime database. The preventive suggestions (before/after) of such cyber offenses has also been embedded so that cyber victims can acquire necessary information once they were affected and can take required actions to get rid of those cruel crimes. The law enforcement official contact address details of concerned state have also been embedded in the Knowledge-Based System. The law enforcement officials perpetually utilize this Knowledge-Based System for the purpose of tackling an intricate assessment making crisis. This system enables the user to instinctively, rapidly, and lithely operate facts to afford an investigative imminent. Data mining mechanizes the exposure of significant cyber crime prototypes in the cyber crime database, utilizing distinct loom and algorithms to stare into present and chronological facts that can then be evaluated to envisage prospect drifts. The escalating possibility to track felony events provides public associations and law enforcement departments the prospect to accumulate and hoard meticulous information, as well as spatial and temporal facts about offense events. Thus, the capability to utilize data investigation tools to extort valuable information associated to immoral events may facilitate law enforcement agencies to better utilize their possessions and extend effectual felony preclusion stratagem (Catlett et al. 2018).

Data visualization is a skill and a type of visual communication that embraces formation and learning of the image depiction of facts. The principal objective of data visualization is to converse information obviously and efficiently by means of numerical grids and plots which facilitate to

evaluate and explain about information along with indication. The Knowledge-Based System affords the formation of cyber crime density maps which facilitate the cyber crime analyst to exploit the offense prototypes. The perceptive prototypes of cyber crime spots were imperative for law enforcement and intellect organizations to probe and thwart cyber crimes. As cyber crimes take place in a region, scrutinizing them through locality and maps facilitate a lot of perceptive. Cyber crime map plots were able to facilitate the offense investigators to discover associations between scandalous in the societal network. As contrast to textual information, image representation of information affords an enhanced perceptive which would be helpful for an individual in perceptive perilous and hazardous regions and it thus can facilitate them to evade such regions and it would also facilitate law enforcement to enhance the refuge in those regions.

Developing maps that enclose cyber crime hotspots were becoming a decisive and prominent tool for cyber crime analyst. These maps were utilized by the cyber crime researchers and forecasters to scrutinize the occasion of cyber crime hotspots in certain regions and why they occur and facilitate them to fabricate the offense hypothesis. It also lets cyber crime researchers to explicate why cyber crimes take place in firm spots and why it does not take place in other locations. Cyber crime analysts would utilize this information to make enhanced assessment, intention possessions, devise tactics and facilitate the law bureau. In the latest era of rising volume of cyber offenses, cyber crime preclusion is at the moment one of the most significant universal concerns, along with the immense distress of spiraling public refuge. The government and area administrators are making an all-out exertion to progress the efficacy of cyber crime preclusion. The frequent exploration addressing this issue has been normally engaged authorities of performance knowledge and figures. Recently, the Data mining loom has been exposed to be a practical decision-support mechanism in envisaging and thwarting the cyber crime. To crumb beside cyber attacks, client training must be primed in alliance with government and other confidential organizations.

The intellectual computing routine would craft the finest elucidation of the worldwide optimization issue with a better probability for diverse optimization problems, and the intellectual computation process could be initiated simply with the heuristic rules of logic estimation technique which is straightforward and simple to recognize.

4. Conclusion

The Knowledge-Based System had been developed for Cyber crime data analysis. To accomplish this, the IT and IPC sections of Cyber crime types of existing Cyber crime cases in India were collected and fed in to the system along with the information of penalty, punishment, preventive suggestions of such cyber offenses. Thus the proposed system would provide a novel tool for visualizing the preceding cyber crime hot spots on maps and could envisage the prospect offenses that may take place. The interactive and image aspects have been supportive in discerning and scrutinizing the cyber crime networks. These would make it probable to exemplify how the hazard of meticulous types of Cyber crimes or offenses diverges across the region, and whether it augments or reduces in the long term.

REFERENCES

- Alavi, M. & Leidner, D. E. (2001). Knowledge Management and Knowledge Management Systems. *MIS Quarterly*, Vol 25 (1), pp 107-136.
- Darek, N. and Jain, H. (1991). The relevance of ES technology for India: A Transponder Perspective. *CSI Digest*, Vol 3(1), pp 68.
- Malleson, N., Heppenstall, A. and See, L. (2010). Crime reduction through simulation: An agent-based model of burglary. *Computers, Environmental and Urban Systems*, Vol 34(3), pp 236-250.
- Nasar J. L and Fisher, B. (1993). Hotspots of fear and crime: A multi-method investigation. *Journal of Environmental Psychology*, Vol 13(3), pp 187-206.
- Wang, T., Rudin, C., Wanger, D and Sevieri, R. (2013). Learning to detect patterns of crime. *Joint European conference on Machine learning and Knowledge discovery in databases*, Springer, pp 515-530.
- Dilek, S., Cakir, H and Aydin, M. (2015). Applications of Artificial Intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence & Applications*, Vol 6(1), pp 21-39.
- Ozgul, F. (2013). Incorporating Data and Methodologies for Knowledge Discovery for Crime. *Elsevier-Intelligent Systems for Security Informatics*, pp 181-197.
- Pande, V. and Sindhu, V. S. (2016). Crime Detection using Data Mining. *International Journal of Engineering Research & Technology*, Vol 5(1).
- SaiVineeth, K. R., Pandey, A., and Pradhan, T. (2016). A Novel Approach for Intelligent Crime pattern discovery and Prediction. *Proceedings of International Conference on Advanced Communication Control and Computing Technologies*, pp 531-538.
- Catlett, C., Cesario, E., Talia, D. and Vinci, A. (2018). A Data-Driven Approach for Spatio-Temporal Crime Predictions in Smart Cities. *IEEE International Conference on Smart Computing (SMARTCOMP)*, pp 17-24.
- Bogahawatte, K. and Adikari, S. (2013). Intelligent Criminal Identification System. *The Eighth International Conference on Computer Science & Education*, pp 633-638.