REAL TIME CRIMINOLOGY DETECTION AND CRIMINAL IDENTIFICATION (RCDCI) ALGORITHM

C.Jayapratha[1], Dr.J.M. Gnanasekar[2]

Abstract— **In our Tamilnadu criminology department we require more efficient and enhanced techniques to improvise on spot crime detection and swift criminal identification methodology. In real time criminal based activities crime rate increases although technologies too increased in various ways. India after been digitized there are very few people who does not use any new technologies thus all technology requires common installation or login like using mail id login, phone number registration, finger print, face or iris recognition etc. All these details are more than enough to locate a person with government support as these details are kept confidential. In our proposed algorithm for Real Time Criminology Detection and Criminal Identification (RCDCI) Algorithm we provide crime identification and detecting the location of criminal in a swift way. We use multilevel cloud backup database from various sources of technology and with that we can able to analyze crime and detect criminal accurately and efficiently.**

Keywords: Tamilnadu criminology, crime detection and criminal identification, real time crime activities, digitized technologies, Detecting and locating criminals using biometrics

I. INTRODUCTION

Usually crime has been a part of human society where the requirement of law and varied sorts of legislations was felt once crime started the very existence of the human society [1]. There are varied sorts of laws and regulation which fight against the crimes constantly within the society [2]. Crime is each social and economic phenomenon, by that whole human society gets distressed.

The nature of the crime has been conjointly dynamical and diversifying with the expansion and development of the society. Presently, the Government of law took the assistance from several techniques and advancement of science for combating against crime [3]. After several advancements have taken place within the field of rhetorical science that has been welcome within the criminal investigation. A number of such advancements are mentioned as any discrepancies that will have crept in are regretted [4].

We have a tendency to propose an approach for the look and implementation of crime detection and criminal identification for Indian cities victimization data processing techniques [5]. Our approach is split into six modules, namely data extraction (DE), knowledge preprocessing (DP), clustering, Google map illustration, classification implementation [6]. Initial module, Delaware extracts the unstructured crime dataset from varied crime net sources, throughout the amount of 2000–2012. Second module, DP cleans, integrates and reduces the extracted crime knowledge into structured crime instances [7]. We have a tendency to represent these instances victimization of five predefined crime attributes. Safeguard measures are taken for the crime info accessibility. Rest of the module is helpful for crime detection, criminal identification and prediction, and crime verification, severally [8].

In our proposed paper we are going to discuss about crime detection and criminology identification through Association of back up storage database, clustering them along with their access permissions and filters criminal links and locate the escaped criminal and identify their criminal activities by tracking their backup storage.

***C.Jayapratha**, Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India*

***Dr. J.M. Gnanasekar**, Professor, Department of computer science, Sri Venkateswara college of engineering, Sriperumbudur, Kancheepuram, Tamilnadu, India*

II. LITERATURE SURVEY

The Social Network may be a network of collective interactions and private associations. It's a structure that constitutes a collection of social actors (nodes) and affiliation between these actors (Links). We tend to all are enclosed by networks and that we ourselves play a very important role of individual units in a very network of various types of social relationships, biological systems [A. L. Barabasi et al.] [9]. Networks will be actual things in Euclidean space, as an example and wattage grid, internet, roads or subways and neural networks [S. Boccaletti et al.] [10].

Social network analysis may be a technique to analyze the links between nodes [Wasserman et al.]. Social Network Analysis is a current rising space of importance in finance, politics, defense and security. In previous couple of years, it's been seen that researchers gain interest within the study of complicated networks [11]. A posh network may be a network having irregular structures, complicated and dynamically ever changing network with time. The most focus of learning the complicated network is to upgrade the data of analyzing of minor networks to a system of huge networks with thousands or a lot of nodes. Usually network study comes underneath graph theory [M. van Steen] [12].

In differing kinds of issues like most slop drawback, graph coloring drawback, will be solved simply and just like the same this sort of principle are going to be utilized in social network study. In social network study we tend to analyze the connection among the nodes and study their dynamics of behavior and structural changes and its effects.

Synchronization method [Yamir Moreno at el.] provides the technique of coupling the network structure and functions. Like in neuronal system, synchronization is applied for coupling billions of neurons connected with one another and makes a whole network. Social Networking is additionally a posh network like neuronal system i.e. social network has complicated structure, sharing little world and scale free options [13]. Synchronization system want to perceive the relation between complicated network structure i.e. link structure and dynamic activity properties of complicated networks. Once learning several researchers work it will be calculated that synchronization is very addicted to degree of the nodes within the network and freelance network size [C. Zhou et al. (2006)].

Crime detection is analyzed victimization k-means clump that iteratively generates two crime clusters that are supported similar crime attributes. Google map improves image to k-means. Criminal identification and prediction is analyzed victimization KNN classification. Crime verification of our results is finished victimization verifies accuracy of 93.62 and 93.99 at some point of the formation of two crime clusters victimization hand-picked crime attributes. Our approach contributes within the betterment of the society by serving to the investigation agencies in crime detection and criminals' identification, and therefore reducing the crime rates.

III. CRIME DETECTION AND CRIMINAL IDENTIFICATION ANALYSIS

The Social Network Analysis obtaining a lot of attention in last many years. It provides the data concerning numerous network structures and their characteristics. There are numerous activities concerned in crime like traffic violation, structure frauds, kidnapping, murders, etc. the most important challenge before of authorities is a way to effectively analyze the massive quantity of criminal information.

With the assistance of social network analysis we are able to investigate the interaction between groups of nodes. We are able to decide the closeness between the members of a group. Social Network Analysis provides the simplest way to observe the interaction between those styles of peoples that are already concerned in some reasonably criminal cases. As we all know that there's a leader in ever gang. We are able to a ranking list of people's ability of leadership. The leaders within the criminal are bound to return to surface.

Security-relevant knowledge comes in two basic forms events and content. Events are typically captured as flows, log files, and alerts and should be forwarded to an analytic server for correlation and analysis. Communications data that describe network connections and data flows between network parts are a special reasonably event which will be gathered directly from network parts rather than from infrastructure or application log files.

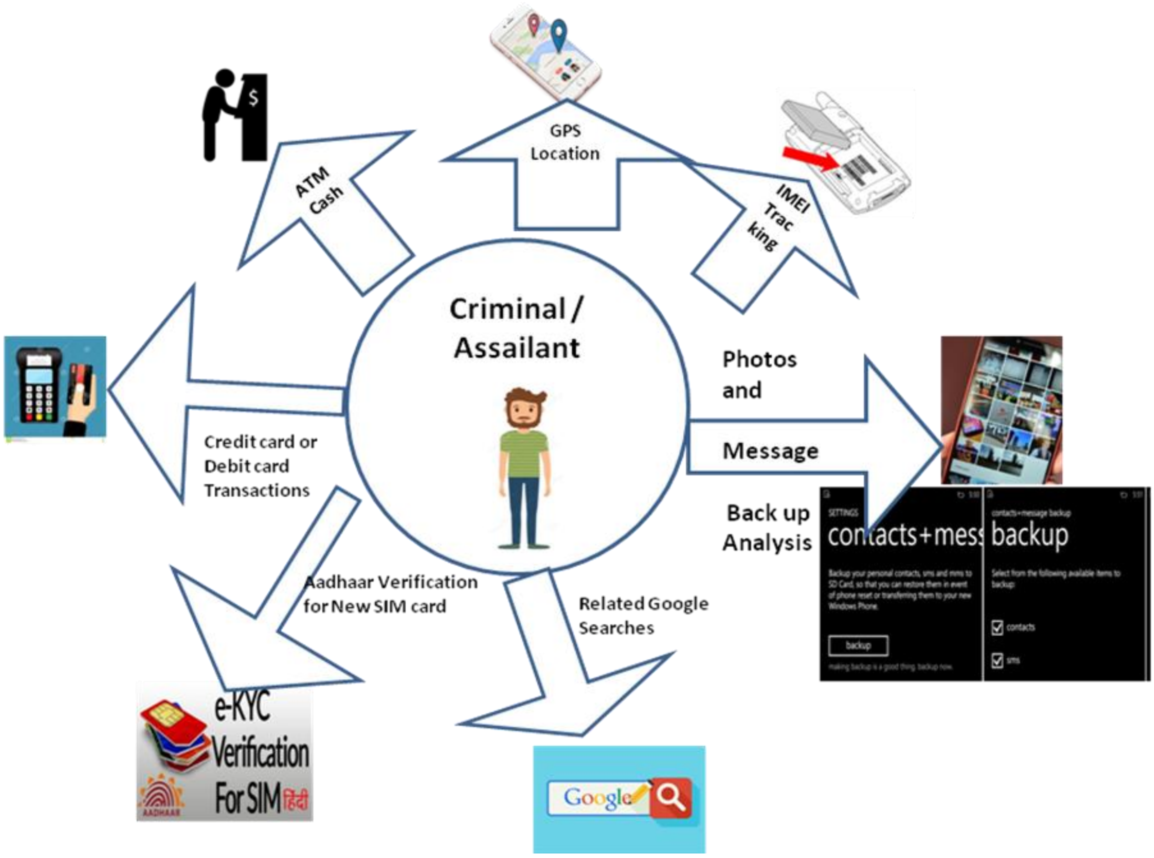
GPS Location
ATM Cash
IMEI Trac king
Criminal / Assailant
Photos and Message Back up Analysis
Credit card or Debit card Transactions
Aadhaar Verification for New SIM card
Related Google Searches
e-KYC Verification For SIM हिंदी
AADHAAR
Google
contacts+mess
backup
contacts
sms

Figure. 1. Criminal Identification Possibilities through his day to day activities.

Event knowledge is beneficial in respondent questions about "what", "when" and "who". Content, such as knowledge files, email, and chat, is typically keep on a service server and should be accessible from this storage purpose for content-scanning analysis. User content also can be gathered directly from information processing networks as packets and re-assembled into sessions for analysis. Content knowledge is best suited to answer specific queries on "what" and "who", and might probably reveal user intent or sentiment. The aspect includes an identity block to emphasize that business executive detection based on cyber measurement is critically captivated with distinguishing the user. For a few knowledge types, investigators may have to correlate multiple identifiers to completely determine the agent. In addition to identity, several business executive detection techniques need the temporal correlation of events like login times, facility entry times, knowledge creation and movement times, etc. To support this sort of correlation, all the information sources (logs, events, content applications, etc.) should be designed with and connected to a universally unambiguous time supply which will be used for time stamping across the enterprise. With the expansion in quality and wireless property, user location info will generally be gathered habitually among the enterprise. This data, once related to with user events, will offer helpful clues to discover probably risky or negligent business executive behavior.

IV Implementation of RCDCI Algorithm And its Advantages

Catching serial criminals could be an intimidating downside for enforcement officers around the world. On the one hand, a restricted quantity of information is out there to the police in terms of crimes scenes and witnesses. However, feat additional knowledge equates to anticipating another crime to be committed that is an unacceptable trade-off. Here we tend to gift a strong and stable geographic profile to predict the residence of the criminal and also the attainable locations of future crime. Our model attracts components from multiple existing models and synthesizes them into a unified model that creates higher use of sure empirical facts of criminology.

Implementation of RCDCI Algorithm will be in various phases and it completely figure out the exact location of the criminal using all google, GPS searches, Facebook location finder apps, IMEI number locator. Even when we buy new SIM card they get Finger print scan and ADHAAR ID so wherever that particular criminals information recorded or used then they are easily cached.

1. There can be a necessary assumption and is that the basis for one amongst the computational elements of our model. We locate them using their mobile GPS, IMEI number etc. The other very important as it ensures that we've enough knowledge to create a correct analysis is to find their finger print recognition or from the back up database in ATM or any CC TV camera footage to find them.
2. The criminal solely resides in one location - By this, we tend to mean that though the criminal might modify their residence, he or she is going to not move to a completely totally different area and commit crimes there. Gives a correct prediction for the situation of the criminal.
3. This is very important because the objective of this model is to find the serial criminal. Obviously, the model cannot provides a definite location of the criminal, but it ought to a minimum of offer enforcement officers an honest plan wherever to appear.
4. Provides an honest estimate of the situation of future crime. This objective is slightly tougher than the primary one, because the criminal will select the location of future crime, to generate a prevention model wherever enforcement will work to prevent future crime.
5. Strong with reference to outliers – Outliers will severely skew predictions such as the one from the centrography model. Honest model can be able to establish outliers and forestall them from adversely moving the computation.
6. Consistent among a given knowledge set that's, if we tend to eliminate knowledge points from the set, they are doing not cause the estimation of the criminal's location to change overly. in addition, we tend to note that if there are eight murders by one serial murderer, then our model ought to provides a similar prediction of the killer's residence once it considers the primary 5, first six, first seven, and every one eight murders. Thus model that doesn't entail excessive computation time. Hence, enforcement is going to be able to get their data more quickly and proceed with the case.

V Conclusion

In our paper we discussed various methods to detect and locate criminals and criminal activities. No person can survive without using any of the existing gadgets, cards, Identity numbers etc. thus with any of the information from the back up database storage we could easily find out that criminal. Thus our algorithm is very helpful and enhances Criminal identification much easier, efficient and accurate.

REFERENCES

[1] S. Chen, B. Mulgrew, and P. M. Grant, "A clustering technique for digital communications channel equalization using radial basis function networks," *IEEE Trans. on Neural Networks*, vol. 4, pp. 570-578, July 1993.

[2] Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. ACM Transactions on Information and Systems Security, 3(3), 186-205.

[3] Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012).

[4] The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technolgy Crimes. Addison-Wesley Professional.

[5] Casey, T. (2007, September). Threat Agent Library Helps Identify Common Security Risks. Retrieved from https://communities.intel.com/thread/49315: https://communities.intel.com/docs/DOC-1151

[6] Casey, T. (2007). Threat Agent Library Helps Identify Information Security Risks. Intel.

[7] Casey, T. (2015). Insider Threat Field Guide. Intel Corporation.

[8] Axelrad, E. T., Sticha, P. J., Brdiczka, O., and Shen, J. (2013). A bayesian network model for predicting insider threats. In Security and Privacy Workshops (SPW), 2013 IEEE, pages 82–89. IEEE.

[9] Barrick, M. R. and Mount, M. K. (1991). The big five personality dimensions and job performance: a metaanalysis. Personnel psychology, 44(1):1–26.

[10] B. Snook, D. Canter, and C. Bennell, "Predicting the home location of serial offenders: A preliminary comparison of the accuracy of human judges with a geographic profiling system," Behavioral Sciences and the Law, 2002.

[11] J. van der Kemp and P. van Koppen, "Fine-tuning geographical profiling," Criminal Profiling: International Theory, Research, and Practice, 2007.

[12] R. Kocsis and H. Irwin, "An analysis of spatial patterns in serial rape,arson, and burglary: The utility of circle theory of environmental range for psychological profiling," Psychiatry, Psychology, and Law, 1997.

[13] J. Warren, R. Reboussin, R. Hazelwood, and J. Wright, "The geographical and temporal sequencing of serial rape," Journal of Interpersonal Violence, 1991.