International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Criminal Profiling using Machine Learning

Aditya Goyal[1], Aime Gupta[2], Alisha Shah[3], Meyga Anne Alexander [4], Aarthi N[5]

[1,2,3,4,5]*Dept. of Computer Science, Vellore Institute of Technology*

Abstract - *The area of digital forensics faces a variety of challenges in sight of the continual broadening of technologies. The authenticity and probity of digital evidence from different areas is additionally an ongoing challenge that needs considerable human interpretation when reconstructing each sequence of events. Expert systems and technologies for AI play a crucial role within the development of tools to support police operations. The systems have proven successful within the areas of raids and entry, enforcement, surveillance of serial criminals, et al. During this paper, we aim to examine and analyze criminal profiling. Criminal behavior and characteristics are identified by analyzing the data using a number of predefined parameters. Crime analysis and prevention can be said as a methodological approach for finding and analyzing patterns and trends in crime. Episodes of cybercrime misusing content-based trickiness talk are expanding because of the ubiquity of instant messages. We use AI and phonetic ways to deal with identifying trickery inside instant messages in cybercriminal systems. This article thinks about the present issue of examination and development of strategy for mental and socio-segment profiles of the guilty party and approval of individual information dependent on the investigation of socio-segment qualities are researched. Such needs are accomplished over 80% feelings like in the created world, logical examinations and confirmation of proof in the courts through digital legal sciences procedures and innovation. While still generally youthful the utilization of computerized legal sciences in criminal examinations is expanding. This has incited law implementation organizations to take a gander at growing more proficient procedures for researching advanced media. Triage devices are viewed as the up and coming age of computerized crime scene investigation investigatory advancements. In any case, such devices are as yet deficient with regards to essential choice help systems, and still require some type of human intercession. The creators propose to utilize a case-based thinking framework to record and store computerized crime scene investigation assessments.*

***Key Words*: Artificial Intelligence (AI), Digital Forensics (DF), Data Mining (DM), Data Recovery (DR), Email Abuse (EA), Hacking (HK), Industrial Espionage (IE), Machine Learning (ML).**

1. INTRODUCTION

This paper deals with criminal profiling. Criminal profiling can be described as a way to interfere with the traits of those responsible for criminal acts. Professionals in the study of criminal profiling have included behavioural specialists, criminal investigators. social scientists, and forensic pathologists [19].

Cybercrime exploits can be divided into "e-enabled" cybercrime and "true" cybercrime. We can describe E-enabled cybercrime as any act of crime that the world knew before the arrival of the World Wide Web but increasingly committed on the Internet. Let's take the example: identity theft or online fraud [20]. True cybercrime can be said as any fraudulent act that will not be present outside of an online environment; for example, denial-of-service attacks or attacks of viruses [21].

Suspicious incidents can be found in many ways. Computer security occurrences are usually recognized in situations where a person doubts that an intolerable or illegal thing has happened that involves the computer networks or data processing equipment of an organization. At first, the action can be reported by an end user, recognized by a system admin, identified by IDS warnings, or found in various other means. Therefore, essentiality is to obtain evidence of digital forensic analysis and its structure of temporary metadata for investigation. The main aim of these investigations is to draw out proofs such as unusual and interesting acts and their causal relationships. Step by step the crime percentage is expanding extensive [22]. Wrongdoing can't be anticipated since it is neither orderly nor irregular. Likewise, the cutting-edge advancements and howdy tech techniques help crooks in accomplishing their offenses. As indicated by Wrongdoing Records Bureau violations like thievery, incendiarism and so forth have been diminished while violations like homicide, sex misuse, assault and so forth have been expanded [23]. The flood in content informing, from one viewpoint, and characteristic vulnerabilities in the Internet engineering driving this method of correspondence is pulling in cybercriminals to abuse unfortunate casualties utilizing this correspondence medium. Two of the procedures cybercriminals use to sidestep content-sifting frameworks to dispatch fruitful cybercrime crusades are: changing successions of dictionaries to make messages one of a kind, and misusing unprotected email customers and couriers on cell phones since these need content channels and so forth [24] .Nowadays present day society is characterized by the web: over a fourth of the total populace is wired into the WWW - and this number is developing each day. The web is a wellspring of data, correspondence, diversion and training, and it is incomprehensible for huge numbers of us to envision a working world without it [25]. They have encouraged commission of customary violations as well as brought forth cybercrimes causing their expansion at a quick

pace. Then again, the informal examination of wrongdoings is bringing about absolutions of violations on an incredibly high scale. The scientific apparatuses neglect to coordinate with the information and strategies of hoodlums. Except if the measurable instruments are overhauled and effective frameworks are created, the danger of expanding absolutions may cause devastation in our general public breaking its financial fabric [26]. This paper talks about a novel way to deal with completing DF assessments; the utilization of information sharing to make a completely computerized investigatory procedure. Advised that Case-Based Reasoning (CBR) permits catch and capacity of DF examiner information that can be reused in an endeavour to recognize the nearness of proof on a type of advanced media. This would permit assessments to embody master information from various sources, instead of getting dependent on one head examiner [27].

2. Literature Survey

Cybercrime has been viewed as discrete as the next logical breakthrough after the advent and apparent success of computer and Internet technology. In equal measure with the privacy, trust, finances and well-being of low-income individuals and organizations, the crisis showed no sign of slowing down [2]. Insufficient investigative techniques, amongst others, are identified because the obstacle to effectively containing cybercrimes [1]. Cyber infrastructures are highly vulnerable to intrusions and other threats. Physical devices and human intervention aren't enough for keeping track of and shielding of these infrastructures; hence, there s a need for more advanced cyber defense systems that require to be flexible, adaptable and robust, and prepared to detect an honest kind of threats and make intelligent real-time decisions[3].Over a period of sometime internet has become the indispensable a neighborhood of human life. Without proper knowledge and awareness, most are using AI in their daily walks of life. This is often the golden opportunity for hackers to deceive people easily. At times, hackers are also cheating the folks that are having sound knowledge on AI. Therefore, cyber security could also be a mutual problem across the planet. Hackers are becoming smarter day by day and that they are more innovative in creating malicious software to require advantage of the vulnerable data of individuals , organizations and governments[4].Cyber Profiling using Log Analysis and K-Means Clustering uses K-Means clustering on the Log data in order to form 3 different clusters depending on the number of sites and its visitors then based on the clustering results we perform profiling[11].New technique known as deep reinforcement learning combines neural networks and reinforcement learning to predict the hidden links in the network that are hid by the criminals in order to perform profiling we find the patterns and do forensics analysis on it[12].Naïve Bayes theorem predicts the criminal for a particular activity by giving all the information such as date criminal id suspects the criminal hotspots[5].Use of deep neural network and other machine learning techniques to predict the crime hotspots and prediction of crimes are being used widely nowadays as it as it does not require more help of humans and is rather an automatic process[6].Preprocessing to remove missing values and separating the different goals with differentiating features on which we apply decision tree, naive bayes for finding out the hotspots is one of the trending process of criminal profiling[7].Profile for each individual criminal is created on which Fuzzy C-Means is applied to form clusters so that we can read the data and draw conclusions from it this profile creation is very helpful for the future needs of the police and the investigating department[8].This can be clubbed with the K-Means clustering algorithm for clustering various crimes for comparing the results of the analysis and find out the various geographical hotspots of crime which can be plotted in the map and provided to the investigators to concentrate on the certain region so that their space of search can be reduced and limits so crime detection is made easy by this[9].Good database for prediction and finding out the hidden aspects of the case using the Apriori algorithm for predicting the association rules to find the relations among the crimes is very essential for criminal profiling[10].A new method uses ACP for parallel scene analysis in which parallel approach for the real crime scene and artificial crime scene is executed so that both the scenes can be related and we can get more information for profiling[11].

Offender profiling is considered to be a cluster of special features that can uniquely identify a criminal from with respect to the crime incident [12]. Criminal profiling has been classified into two separate models called inductive and deductive profiling. Inductive profiling gathers the data from the general offender database which holds the data of criminals to make an analysis and arrive at a conclusion based on inductive reasoning [12].

Deductive profiling although never relies on general aspects on the sample or experimental groups. It is based on deductive logic reasoning and goes from the specific level to the general level [12].

On a large scale, cybercrimes have advanced to a higher level with the modernization and expansion of technology and the electronic medium. An accurate and specific profile of an inside cybercriminal may help in identifying both prospectively and retrospectively the case behind the criminal [14].

The profiling process involves six stages which are: -

- Profiling inputs
- Decision making process models
- Crime assessments
- Profile analysis
- Investigation of the case
- Apprehension involved behind

This can result in potential identification factors that describe the probable features of the criminal. Identification factors include sex, type of employment, race, ethnicity, residential proximity or closeness, type of transportation involved,

social-development age, motive behind the crime scene and many others [15].

Cybercrime profiling in this paper is based on four dimensions, namely breadth, depth, vulnerabilities and data collection tools (e.g., honeypots) and cybercrime-cybercriminal correlation. Cybercrime includes the usage of computer networks and infrastructure for committing crimes or any criminal offence committed against someone with the help of a computer network.

Breadth is a metric that is used to measure or calculate the scope or range of infiltration of the attack or cybercrime. The paper has provided two key abstractions of depth involving host breadth and network breadth. The host breadth measures the scope of infiltration or resistance on a single host while the network breadth measures the scope or possibility of an infiltration on the host network. Host and network breadth can both be measured through network connection analysis.

Depth has been used in a similar way to breadth, although its focus is to calculate the extent or degree of resistance or infiltration of the network intrusion. Let us understand the two abstractions of depth. Host depth shows the level to which an infiltration penetrates the host node; and providing a general or less-specific determination of the host penetration involved. Service depth, on the other side, measures the degree of infiltration of a particular service; this is highly capable of revealing more detailed and specific information concerning the exact and accurate activities conducted by the attacker [16].

A lot of vulnerabilities are there in the system that allows an attacker to compromise it. When used in conjunction with elements such as sophistication and attackers, the amalgamation can be used to increase the precision of the cybercrime profile. The final aspect of cybercrime profiling is the digital forensics tools. Often the tools are simply perceived or considered as the software part that is utilized to exploit vulnerabilities existing in the system. Although this paper consists of both the software and all the hardware that is used in an attack. On software, it includes root kits, backdoors, attack scripts and innocuous software like FTP, SSH, PING and WGET. Hardware includes the attacker's system and their internet connection [18].

Text mining has been proposed as a solution for criminal profiling in this paper. It is based on the calculation of Euclidean similarity distance to differentiate the suspicious elements. The following processes are involved:

- Text corpus: a complete collection of all keywords in the data.
- Corpus processing is done taking into consideration the account indicators
- Detection of events and trending topics
- Prediction of the criminal activities
- Classification process using the similarity approach [17].

In nations like England, Cambridge Police Department have done a comparative one named Series Finder for finding the designs in robbery. To accomplish this, they utilized the modus operandi of the guilty party and they extricated some wrongdoing designs which were trailed by the guilty party. The calculation builds the usual way of doing things of the guilty party. The M.O. is a lot of propensities for a crook and is a sort of conduct used to describe a design. The information included methods for section (front entryway, window, and so on.), day of the week, attributes of the property (loft, house), and geographic nearness to different break ins. Utilizing nine known wrongdoing arrangements of robberies, Series Finder recouped the majority of the wrongdoings inside these examples and furthermore distinguished nine extra wrongdoings. The anticipated outcome appeared over 80% precision. So, a similar idea we are applying here for example discover obscure examples from known information and realities. It's the primary scientifically principled way to deal with the mechanized learning of wrongdoing arrangement. identified with wrongdoings like theft we can extricate the rundown of weapons guilty party utilized while perpetrating the wrongdoing. We have incorporated an idea called Coreference Resolution to discover the referenced elements in a book. In etymology, Coreference happens when at least two articulations in a book allude to the same individual or thing for example in the event that they have a similar referent. For prediction of crimes we are using the choice tree idea. A choice tree is like a diagram in which the interior hub speaks to test on a trait, and each branch speaks to the result of a test. The principle bit of leeway of utilizing choice trees is that it is easy to comprehend and decipher. The other focal points incorporate its powerful nature and furthermore it functions admirably with enormous informational collections. This element causes the calculations to make better choices about factors [23]. Cybercrime in content-based correspondence can be likewise recognized utilizing PL highlights. This is on the grounds that semantic conduct in content-based correspondence can be mapped to criminal mental procedures. Instruments like Linguistic Inquiry and Word Count (LIWC) have been broadly utilized in contemplating different connections among brain science and phonetics. LWIC underpins various semantic forms for different mental procedures; we distinguish highlights which are significant to tricks and extortion in instant messages. For example, phonetic highlights like word amount, normal sentence length, first-individual solitary and restrictive words have a relationship with mental procedures like loquacity, intellectual intricacy and honesty, separately. We gather instant messages from two web classifications: Facebook and email, in light of the fact that these correspondence mediums are offbeat and instant messages don't have tremendous phonetic varieties. The information we use to distinguish and break down substance based digital wrongdoing is genuine word information and it has issues like: commotion, missing qualities, irregularity, and repetition, subsequently it must be preprocessed [24]. The making of the individual mental profile of the web-character is the one of the most significant phases of the calculation. The web-character mental profile is a portrayal of the possible character, conduct, issues and interests of an

individual or web-character that depends on mental techniques. Mental profiling might be portrayed as a technique for suspect ID which tries to distinguish an individual's psychological, passionate, and character qualities. The information on mental idiosyncrasies of digital criminal advances the right examination of wrongdoing comprehending issues in the field of digital wrongdoing. The principle segments of the structure are the accompanying elements: Hereditarily and natural elements. The closest social condition Individual and mental qualities. Childhood of minors in single-parent families (absence of a parent); deserts in family life, particularly in the ethical environment of family connections; insufficiencies in the relationship of guardians and youngsters, which are communicated most unmistakably in the wonders of vagrancy. Taking a stab at exhibit the fortitude, boldness and immovability to individual; preposterous and dead sincere to make an activity that is communicated in crazy socially perilous act Digital guilty party is: complex framework with solid and sharp enough protests, differences and alternate extremes; irregularity of practices, inside shaky framework with strongly communicated reliance on the circumstance; the circumstance is normally described by the contentions that require brisk choices dependent on good and lawful standards [25]. There are no conventional benchmarks, methodology nor models for computerized crime scene investigation to which courts can allude. The current models center around one part of the procedure. It ought to depict the whole lifecycle of an advanced criminological examination. Digital measurable proof gathered in one nation isn't acceptable in remote courts. Government approaches and digital laws from various locales should put forth attempts to determine clashes and issues emerging due to multi-locale examinations. There is a necessity for preparing examination organizations and legal individuals. There exists a need to create examination methods like Digital Forensic Examinations to gather computerized proof and to correct Indian Cyber laws to coordinate the speed of innovative advancement. According to the information of the National Crime Record Bureau, given by the creator of, during recent years, the enrolled cases under IT Act are 3682 and the conviction rate is 7% for example the enlisted cases are expanding and the conviction rate is declining. The expansion in detailed cases is multiple times. As per Supporter Pawan Duggal, a digital wrongdoing master and senior promoter of the Supreme Court, more often than not electronic proof is neither caught in the correct manner nor is it held and safeguarded in the way required to be helpful in law. According to the NCRB report of 2015-16, the cybercrimes in India are constantly expanding, however in light of incapable examination, the level of understood cases is low. Inspects criminal equity reactions to digital wrongdoing under the normal law model. The Comprehensive Study on Cybercrime has been done and it centers around center issues of concern. The paper talks about different obstructions to cybercrime examinations, indictments and advanced legal cross examinations like inadequacy in following lawbreaker movement when information anonymization and muddling strategies have been utilized. Accessibility of information sterilization and gadget cleaning programming for purchaser gadgets may prompt decimation of proof. There exists powerlessness to get approval for leading on the web investigation and assortment of remotely put away information especially if the base station is outside the ward of the neighborhood specialists and powerlessness to get information because of headways in buyer security on product gadgets like solid encryption, open source security instruments and hostile to legal advances. Rising information assurance and protection laws overall are putting electronic data past the compass of exploring specialists. Various approaches that spread all PC legal examination steps viz. imaging, examination and introduction ought to be utilized. The development in the quantity of cybercriminal entertainers and chances to take part in profoundly beneficial criminal operations is the primary driver which has offered access to the advancement of new cybercrime apparatuses in territories, for example, ATM misrepresentation and portable malware. A huge piece of the issue is identified with poor computerized security measures and practice by organizations and people [26]. A CBR framework chooses a case from its information base that fits best to make an answer. New cases are completely added to the information base to build its ability for making arrangements. CBR frameworks are reliant on the cases they hold in their information base to perform to the most elevated level [18]. Salomos way to deal with CBR frameworks is one that fits well inside the working standards of DF. This is like the manner by which people issue explanations, when a superior or more productive strategy is found to tackle an issue, the old repetitive strategy is evacuated. A comparative rule can be seen in DF, when improved strategies are created, other techniques are never again utilized. The impediments of evacuating excess cases are that should an issue require an old arrangement, the information base is never again able to complete the assignment as it doesn't have the information. CBR frameworks can deal with complex information for multifaceted issues and demonstrate value in fields where there are enormous assortments of unstructured information. One of the principal issues looked at during the production of a KB for this theory is that most KBs store sections of realities concerning the subject and not a total arrangement. When utilizing a KB for DF examinations, a more prominent detail of information would be put away. For instance, it isn't adequate for a KB to just distinguish Internet perusing history on a suspect machine. Such history must be examined and arranged to see in the event that it is applicable. There is likewise almost no possibility when doing DF examinations that an immediate match will happen. Numerous KBs record data in a configuration which can be questioned with genuine or bogus qualities. In numerous DF examinations, applicable information shifts in detail, along these lines a fluffy match most happen. KBs are regularly inadequate as a total arrangement as well numerous issues include a vast measure of information which is basically unrealistic to actualize [27].

3. Survey Table

Name	DF	ML-AI	EA	DM	HK	DR	IE	Year
[19]	Yes	Yes	No	No	No	No	No	1998
[15]	Yes	No	No	No	No	No	No	1999
[12]	Yes	No	No	No	No	No	No	2000
[13]	Yes	No	No	No	No	No	No	2003
[14]	Yes	No	No	No	No	No	No	2005
[16]	Yes	No	No	No	No	No	No	2008
[20]	Yes	No	Yes	No	No	No	No	2008
[4]	No	Yes	No	Yes	No	No	No	2013
[25]	Yes	No	No	No	No	Yes	No	2013
[18]	Yes	No	No	No	No	Yes	No	2014
[22]	Yes	No	No	No	No	No	No	2014
[23]	Yes	Yes	No	Yes	No	No	No	2014
[3]	Yes	Yes	No	No	No	No	No	2015
[17]	Yes	Yes	No	Yes	No	No	No	2015
[7]	Yes	Yes	No	Yes	No	No	No	2015
[8]	Yes	Yes	No	Yes	No	No	No	2016
[24]	No	Yes	No	Yes	No	No	No	2016
[1]	Yes	No	No	No	No	No	No	2017
[10]	Yes	Yes	No	Yes	No	No	No	2017
[5]	Yes	Yes	No	Yes	No	No	No	2017
[2]	Yes	No	No	No	No	No	No	2018
[9]	Yes	Yes	No	No	No	No	No	2018
[11]	Yes	Yes	No	No	No	No	No	2018
[26]	Yes	No	No	No	Yes	No	No	2018
[6]	Yes	Yes	No	Yes	No	No	No	2019

4. CONCLUSIONS

With the advancement of technology, cybercrimes have increased to a great extent. Cybercrimes are often overlooked by criminal profiling. An accurate and specific profile of a cybercriminal may help in identifying the case behind the criminal. The role of criminal prosecution as an important investigative tool in traditional cases, and as its contribution to improving investigations and cybercriminal findings, has been highlighted. Profile for each individual criminal is created on which Fuzzy C-Means is applied to form clusters so that we can read the data and draw conclusions from it this profile creation is very helpful for the future needs of the police and the investigating department. This can be clubbed with the K-Means clustering algorithm for clustering various crimes for comparing the results of the analysis and find out the various geographical hotspots of crime which can be plotted in the map and provided to the investigators to concentrate on the certain region so that their space of search can be reduced and limits so crime detection is made easy by this. Bad behavior data is a sensitive and immense space and right now needs some powerful packing frameworks and computations which will help the bad behavior examiners and law specialists recuperate the data and information and draw in models and near a result which will bolster their assessment. The package batching figuring can be made with the goal that settles the unsolved bad behaviors faster. Package gathering is especially steady to draw patterns and best procedure for finding closeness measures. This paper deals with the unmistakable examination of bad behavior data assessment using data mining and gathering and its huge procedures.

ACKNOWLEDGEMENT

We are sincerely thankful to Vellore Institute of Technology for providing us the opportunity to write a paper in the form of a dissertation on the topic Criminal Profiling. We are also thankful to our faculty in charge Mr. Anand Kumar for guiding us in every stage of this paper. Without his support it would have been very difficult for us to prepare the paper so informative and interesting. Through this paper we have learnt a lot about criminal profiling and about its various methods using Machine Learning. We hope this paper inspire young minds and could be useful for future innovations.

REFERENCES

[1]A. M. Balogun and T. Zuva, "Open issues in cybercriminal profiling," 2017 1st International Conference on Next Generation Computing Applications (NextComp), Mauritius, 2017, pp. 141-145.
[2]Balogun, A.M. and Zuva, T., 2018, December. Criminal Profiling in Digital Forensics: Assumptions, Challenges and Probable Solution. In 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC) (pp. 1-7). IEEE.
[3]Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.
[4]K. Bogahawatte and S. Adikari, "Intelligent criminal identification system," 2013 8th International Conference on Computer Science & Education, Colombo, 2013, pp. 633-638.
[5]Vural, M. S., & Gök, M. (2017). Criminal prediction using Naive Bayes theory. Neural Computing and Applications, 28(9), 2581-2592.
[6]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.
[7]Saeed, U., Sarim, M., Usmani, A., Mukhtar, A., Shaikh, A. B., & Raffat, S. K. (2015). Application of machine learning algorithms in crime classification and classification rule mining. Research Journal of Recent Sciences ISSN, 2277, 2502.
[8]Adeyiga, J. A., Adeyanju, I. A., Olabiyisi, S. O., Omidiora, E. O., & Bello, A. (2016). An improved fuzzy C-means clustering algorithm framework for profiling criminal. Advan. Multidisc. & Scientific (AIMS) Res. J, 2(2), 123-134.
[9]Vaidya, O., Mitra, S., Kumbhar, R., Chavan, S., & Patil, M. R. (2018). CRIME RATE PREDICTION USING DATA CLUSTERING ALGORITHMS. International Research Journal of Engineering and Technology (IRJET) e-ISSN, 2395-0056.
[10]Sevri, M., Karacan, H., & Akcayol, M. A. (2017). Crime analysis based on association rules using apriori algorithm. International Journal of Information and Electronics Engineering, 7(3), 99-102.
[11]Wang, S., Wang, X., Ye, P., Yuan, Y., Liu, S., & Wang, F. Y. (2018). Parallel crime scene analysis based on ACP approach. IEEE Transactions on Computational Social Systems, 5(1), 244-255.
[12] - Canter, D. (2000). Offender profiling and criminal differentiation. Legal and Criminological Psychology, 5(1), 23□46. doi:10.1348/135532500167958
[13] - Rogers, M. (2003). The role of criminal profiling in the computer forensics process. Computers & Security, 22(4), 292□298. doi:10.1016/s0167-4048(03)00405-x
[14] - Nykodym, N.,Taylor, R.,Vilela,J.(2005)Criminal profiling and insider cyber crime.Computer Law and Security Report, 408-414.doi:10.1016/j.diin.2005.11.004
[15] - COOK, P. E., & HINMAN, D. L. (1999). Criminal Profiling. Journal of Contemporary Criminal Justice, 15(3), 230□241. doi:10.1177/1043986299015003002
[16] - Kwan, L., Ray, P., & Stephens, G. (2008). Towards a Methodology for Profiling Cyber Criminals. Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). doi:10.1109/hicss.2008.460
[17] - Alami, S., & Elbeqqali, O. (2015). Cybercrime profiling: Text mining techniques to detect and predict criminal activities in microblog posts. 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA). doi:10.1109/sita.2015.7358435

[18] - Silde, A., & Angelopoulou, O. (2014). A Digital Forensics Profiling Methodology for the Cyberstalker. 2014 International Conference on Intelligent Networking and Collaborative Systems. doi:10.1109/incos.2014.118
[19] Brahan, J. W., Lam, K. P., Chan, H., & Leung, W. (1998). AICAMS: artificial intelligence crime analysis and management system. Knowledge-Based Systems, 11(5-6), 355-361.
[20] Arthur, K. K., Olivier, M. S., Venter, H. S., & Eloff, J. H. (2008, March). Considerations Towards a Cyber Crime Profiling System. In 2008 Third International Conference on Availability, Reliability and Security (pp. 1388-1393). IEEE.
[21] Karyda, M., & Mitrou, L. (2007, August). Internet forensics: Legal and technical issues. In Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007) (pp. 3-12). IEEE.
[22] Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. Information Security Journal: A Global Perspective, 23(4-6), 172-178.
[23] Sathyadevan, S., S, D. M., & Gangadharan, S. (n.d.). (2014) Crime Analysis and Prediction Using Data Mining. Crime Analysis and Prediction Using Data Mining.
[24] Mbaziira, A. V., & Jones, J. (2016). A Text-based Deception Detection Model for Cybercrime. A Text-Based Deception Detection Model for Cybercrime.
[25] Fedushko, S., & Bardyn, N. (2013). ALGORITHM OF THE CYBER CRIMINALS IDENTIFICATION. Global Journal Of Engineering, Design & Technology
[26] Mishra, U. S. (2018). Application of Cyber Forensics in Crime Investigation, 5(3).
[27] Horseman, G., Liang, C., & Vickers, P. (2011). A Case Based Reasoning System for Automated Forensic Examinations .