Journal of Cyber Security

Tech Science Press

DOI: 10.32604/jcs.2022.038791
Article

Discovering the Common Traits of Cybercrimes in Pakistan Using Associative Classification with Ant Colony Optimization

Abdul Rauf[1], Muhammad Asif Khan[1,*], Hamid Hussain Awan[2], Waseem Shahzad[3] and Najeeb Ul Husaan[4]

[1]Department of Computer Science & IT, Sarhad University of Science & Information Technology, Peshawar, 25000, Pakistan
[2]Faculty of Computer Science, IBADAT International University, Sihala, Islamabad, 45750, Pakistan
[3]School of Computing, National University of Computer and Emerging Sciences, Islamabad, 44000, Pakistan
[4]Department of Computer Science, Network Home Institute of Information Technology, Multan, 60700, Pakistan
*Corresponding Author: Muhammad Asif Khan. Email: masifhamzallah@gmail.com
Received: 29 December 2022; Accepted: 10 April 2023; Published: 10 August 2023

Abstract: In the modern world, law enforcement authorities are facing challenges due to the advanced technology used by criminals to commit crimes. Criminals follow specific patterns to carry out their crimes, which can be identified using machine learning and swarm intelligence approaches. This article proposes the use of the Ant Colony Optimization algorithm to create an associative classification of crime data, which can reveal potential relationships between different features and crime types. The experiments conducted in this research show that this approach can discover various associations among the features of crime data and the specific patterns that major crime types depend on. This research can be beneficial in discovering the patterns leading to a specific class of crimes, allowing law enforcement agencies to take proactive measures to prevent them. Experimental results demonstrate that ACO-based associative classification model predicted 10 out of 16 crime types with 90% or more accuracy based on discovery of association among dataset features. Hence, the proposed approach is a viable tool for application in forensic and investigation of crimes.

Keywords: Crime; law-enforcement agencies; machine learning; swarm intelligence; ant colony optimization; associative classification

1 Introduction

The world as a whole is benefiting from cyber technology and applications. The word "cybercrime" also referred to as "cyber-space offences" is a complex term covering a broad range of crimes against human, humanity and machines. It is a serious threat to the world economy, human safety and society. It is obligatory to devise systematic approaches to cope up with the cybercrime incidents [1].

The threats faced by the electronically connected world have made countries realize that it is not just a technological instrument. Rather a primary strategic tool used by state actors or non-state actors

to impair a functioning economy or leave the command-and-control system of the military in serious disarray in the middle of the war. It was inevitable as technology became more pervasive [2]. Cyber security is an issue that has captured the world's attention for almost three decades now. Recent cyber-attacks and increasing cybercrimes have earned center stage in the military and security doctrines of significant military and economic powers. Countries like the United States (US), the United Kingdom (UK), Canada, Australia, India, Turkey, and states like Pakistan have set Cyber Security policies. Pakistan announced its Cyber Security Policy to counter the emerging challenges of cyber-attacks that may be launched on its critical infrastructure and critical information infrastructure, which will be considered an act of aggression. Iran also is working on a Cyber defense development program [3].

Cybercrimes as a political tool suggest dangerous trends in the international political system. On top of that, state and non-state actors always want to steal the vulnerable data and strike the state's interests to achieve their political and strategic interests. Likewise, the industrial control system could face a sophisticated attack that can potentially harm public safety by shutting down or affecting a public utility [4]. New technologies and information regimes have affected warfare methods and means, including bringing new dimensions of net-centric warfare. At present, communications and information technologies may transfer geopolitical and geostrategic landscapes. Importantly, these technologies have brought significant transformation, including the dawn of cyber security. The present-day world is cognizant of this new emergence [5]. The two major categories of cyber-crimes include computer-assisted and computer-focused cybercrimes. Money laundering, fraud, child pornography, intellectual property theft, and drug trafficking are the few examples of computer-assisted cybercrimes. On the other hand, computer-focused cybercrimes include website defacement, hacking, computer exploits, denial of service attack (DOS attack), and phishing [6].

In 1960s, computers codes were modified is termed as the first cybercrime [7]. The first computer worm was developed in 1988 at Massachusetts Institute of Technology by Robert T. Morris [8]. The Russian hackers in 1994 made transactions of huge amount to bank accounts at United States, Germany, Russia, Switzerland and Netherlands [7]. In critical and complex infrastructures such as power grids, navigation systems, and transportation systems, a networked control system plays a major role. Malicious attacks have a greater chance to destroy the communication settings during exchange of data among sensors and other network components due to lack of technical and physical resources. A novel attack detection approach is developed based on the ellipsoid estimation to meet the challenge of cyber-attacks in a networked control system [9]. The cyber-physical systems are one of the soft targets for the attackers where malicious attacks and unknown input can dysfunction the sensors by modifying the genuine data to arbitrary ones. A sliding mode observer is designed to eliminate the effect of malicious attacks and unknown input [10]. The air conditioning system in a European bank was attacked in 2005 to shut down the computer system due to increase in temperature. Cyber warfare is a form of warfare that is fought without weapons. It is performed illegally by an individual, organization or group of hackers that can cause political instability, economic crises among countries [11]. In 2015, electrical power was shut down because of malicious attacks in Ukraine. As a result, more than 200,000 customers, 50 substations and three regional electrical power distribution companies were affected [12].

Remote disconnection is one of the techniques used by the attackers to disconnect the uninterruptable power supply system [13]. These attempts not only slow down the systems but stop the recovery processes [12]. The users face login failure despite being the authentic users of the system. Cyber-bullying is a kind of cybercrime that targets the psychological health of a person, identity and credit card theft [14]. One of the most popular cybercrimes is phishing [15]. Attackers trick users into

providing their sensitive information through a fake link website [12]. To avoid phishing attacks, ignore the links that are provided in suspicious emails and visit only safe websites with "https" [16].

The attackers through SQL injection attacks harm the databases with the help of applying SQL queries. They can access, alter and delete the databases [17]. The most frequent attack is the Denial-of-service (DoS) attack, in which the online services get compromised. The attackers put large numbers of fake requests crashing the system and stop the provision of their intended services to the legitimate users. The most severe attack is the distributed denial-of-service (DDoS) attack, where the victim becomes an attacker such as zombie [18]. Implantable Medical Devices (IMDs) are the electronic devices used for disease control inside the human body. They often have threats with respect to its security. It can cause serious consequences to patient's health if targeted by the attackers [19]. Detection and prevention of cyber-attacks is possible when a vigilant system analyze the social and internet traffic. The contribution of machine learning is significant while replacing the manual systems with automated approaches. In this context, a data-driven cyber security system has been devised and adopted for social and internet traffic analysis to broaden the scope towards cyber security where human, society, and assets are the potential targets [20].

In an era of ever-increasing crime data, it is essential for cyber experts to unearth hidden patterns, and reveal implicit relationships between data, so as to facilitate the law enforcement authorities and security agencies to predict crime occurrences and track down potential criminals.

The proposed approach plays a vital role of discovering patterns or habits adapted by criminals while committing crimes. This is achieved by discovery of associativity among features like area of crime commitment, gender, of the criminal technology sed, etc. The motivation for the study is that criminals usually follow same traits for the same type of crimes. Hence, prediction of future crimes is expected to be much easier than before with the help of the proposed approach. Experimental results show that AC-ACO comprehensively outperformed Ant Miner [21] and the Random Forest (RF) [22] algorithms. Ant Miner is an Ant Colony Optimization implementation that works like AC-ACO except that it does not utilize association among features of the underlying dataset. The reason for choosing Ant Miner is to prove the power of associativity among features of the provided data. Random Forest is a widely-used classification algorithm for classification of rule-based classification models.

The remainder of this article is organized as follows. Section 2 introduces the cybercrimes and Pakistan. The background of the crime prediction approaches are highlighted in Section 3. Section 4 gives the proposed methodology to map patterns in the underlying dataset for the crime type. Section 5 provides a comprehensive description of the dataset used. Experimental results based on the crime data of several typical areas and cities in Pakistan are discussed in Section 6. Section 7 provides the conclusion and important future recommendations are required to adhere to this Microsoft Word template in preparing their manuscripts for submission. It will speed up the review and typesetting process.

2 Cyber Crimes and Pakistan

Companies were heavily reliant on human resources several years ago, but with the rapid growth of technology, computers have now fully displaced humans. The human race has been revolutionized through new technology, discoveries, and innovations. From the invention of the computer for various reasons two decades ago to today's current system of networking and usage, computer became an enormously important aspect of every man's life. Cybercrime, often known as electronic crime, is a vast and ever-expanding issue. It has no limits. There is no precise definition of cybercrime. In Pakistan, cybercrime has escalated during the last two decades. We lacked digital forensic and information data

specialists. There was no recent system accessible. There had no cybercrime legislation in Pakistan until the government approved the Prevention of Electronic Crimes Act (PECA) in 2016 [23].

2.1 Origin of Cyber Crime

In the 1970s, a group known as "phreakers" formed in America. They would perpetrate crimes through telephones. A well-known member of the group was John Draper. This group would employ tones similar to those used in American telephony to make free calls. Some researchers believe that the history and origins of cybercrime may be traced back to ARPANET (Advance Research Projects Agency Network) [7]. The US Department of Defense supported the initiative. Its primary goal was to provide secure communications for military use. Using the same method, communications may be broken into packets and reconstructed in their original state.

When a group of exceptionally experienced computer programmers began to assault telephones in the telecommunications industry, the word "hacking" became widely known. Phreakers were a group of extremely adept computer programmers. They were able to access the system and figure out how to call for free in several ways. They discovered ways for anyone who knows the system to call for free wherever they wish. A undercover operation was carried out by an American investigating agency in which various data storage devices and operating systems were retrieved. Different hackers utilized these devices for free calls and various types of card fraud. Despite varying penalties in various jurisdictions, cybercrime is a rapidly growing concern.

2.2 Pakistan's Initiatives

In the 1990s, the internet was made available. Pakistan is among the top Internet-using countries. The internet has made life easier and less time taking, but it has also given rise to theft, fraud, child pornography, extortion, and other crimes. People in Pakistan abuse the Internet, with the most extreme cases including illegal and illicit behavior. For this study, the Federal Investigation Agency (FIA) provided the cyber rimes related data of 2019 to 2022 which has been portrayed in Figs. 1–3. In Fig. 1, the number of complaints received in last four years by the FIA from 2019 to 2022 by different sources are represented.

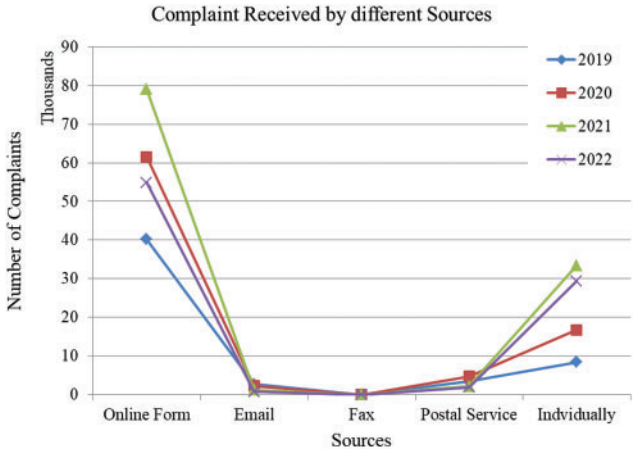
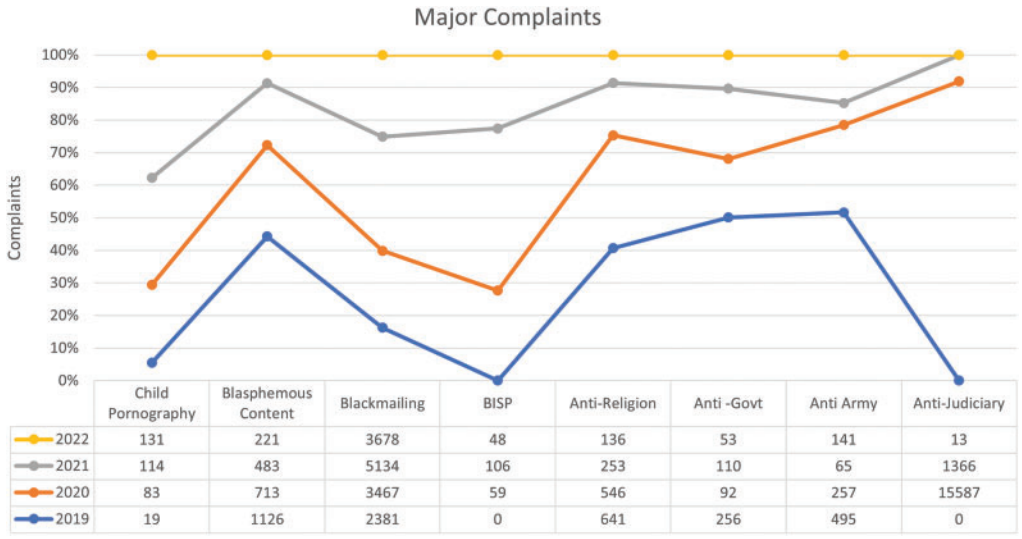


Figure 1: Complaint received by different sources in the years 2019–22



	Child Pornography	Blasphemous Content	Blackmailing	BISP	Anti-Religion	Anti -Govt	Anti Army	Anti-Judiciary
2022	131	221	3678	48	136	53	141	13
2021	114	483	5134	106	253	110	65	1366
2020	83	713	3467	59	546	92	257	15587
2019	19	1126	2381	0	641	256	495	0

Figure 2: Major complaint received in the years 2019–22

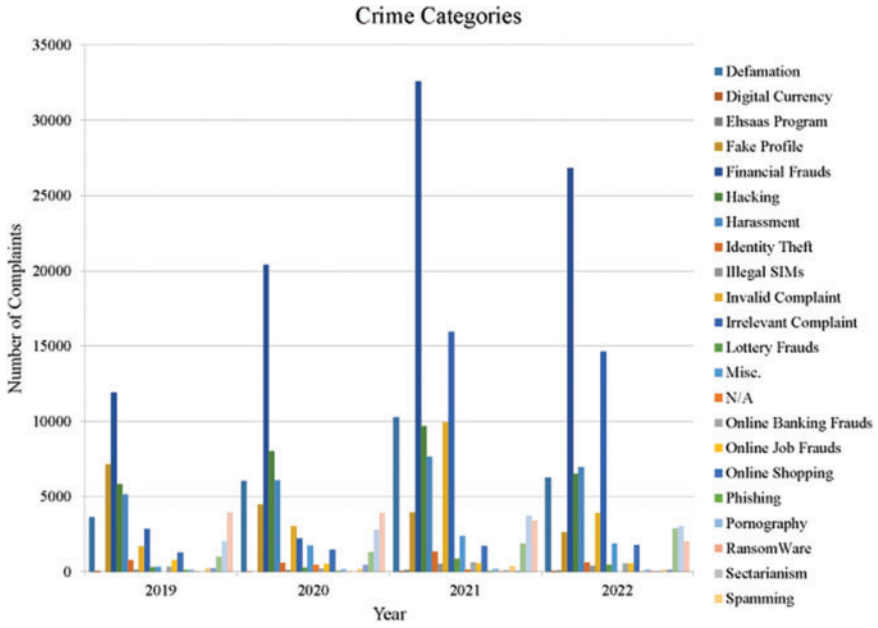


Figure 3: Number of different crimes occurred in the years 2019–22

Figs. 2 and 3 represent the major complaints received and various crime categories reported in last four years by the FIA from 2019 to 2022 by different sources, respectively.

There was no formal procedure, and offenders were frequently released. The government established a national response center for cybercrime under the supervision of the Federal Investigation Agency (FIA). The fundamental reason for its development was to prevent the abuse of the internet. This agency specializes in cyber security, cyber fraud, technical investigation, and digital forensics. In

2003, the first incidence of cybercrime in Pakistan was recorded. Five Pakistanis were engaged in an import and export firm using false information and credit cards.

Fig. 4 shows the investigation work flow of the FIA and detailed view of the complaint dealing process. A separate court for cybercrime is required, and an increase in the number of cybercrime experts. To combat the present crime rate, advanced systems are necessary.

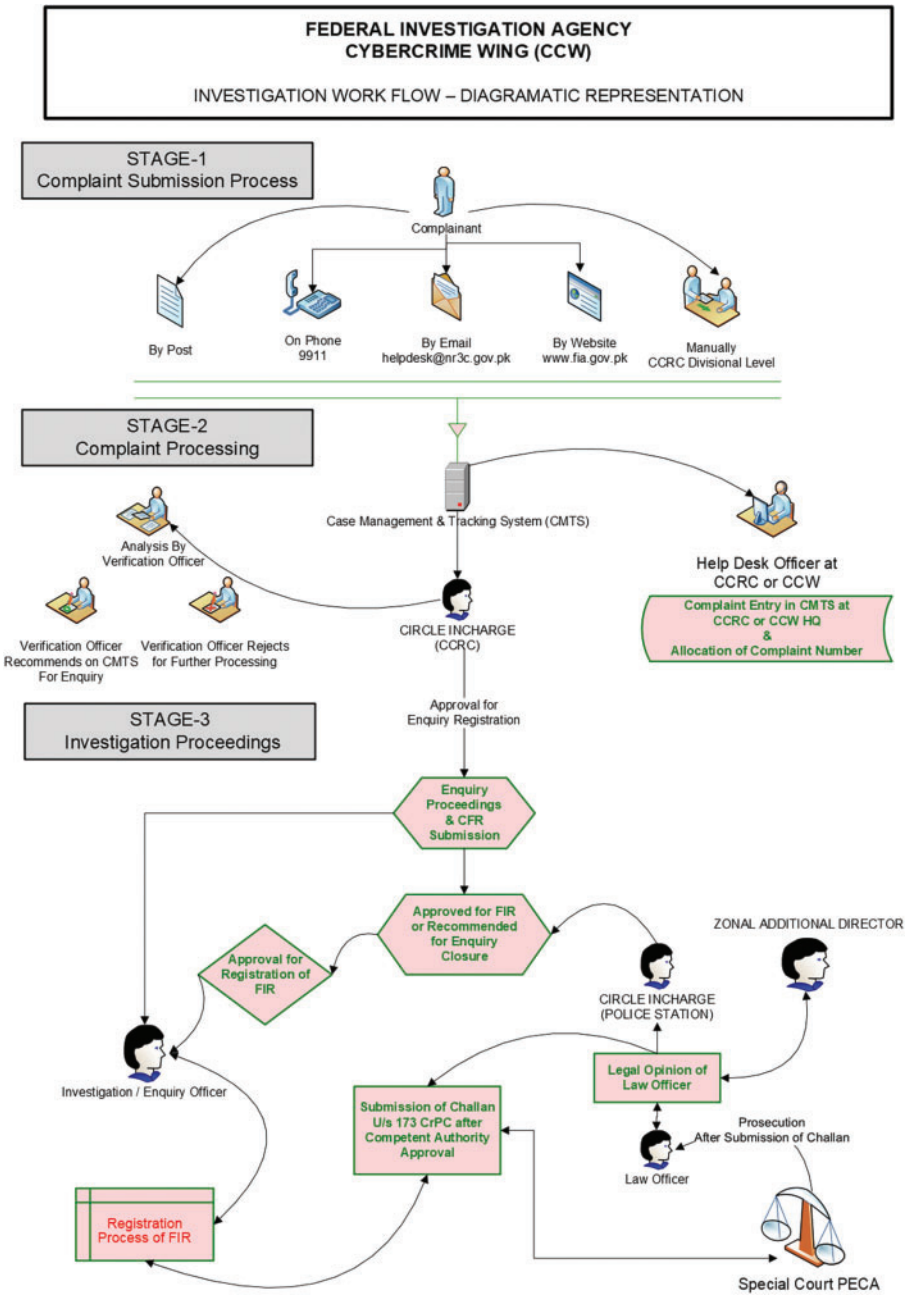


Figure 4: Complaint dealing process by FIA

In 2016, the Prevention of Electronic Crimes Act was approved by the Pakistani government, which includes the offences and penalties. Here are some examples of noteworthy cybercrimes that happen in Pakistan and across the world.

1. *Bank Fraud:* An unlawful and unapproved method of obtaining someone else's money.
2. *Illegal Data Access:* While the penalty for willful unlawful gain, misusing the equipment or data, or agreeing to engage into a relationship with or cause damage to another person is two years in prison or a fine of up to ten million rupees, or both.
3. *Advance Free Fraud:* A common sort of internet scam. Getting your hands on someone else's money used to be difficult, but with technological innovation, it has gotten lot easier. It has gotten lot easier with the aid of the internet.
4. *Cyber Stalking:* It occurs when someone knowingly uses an information system such as the internet, a website, or email to compel or frighten another person by continuously contacting him despite his evident unwillingness, or monitoring the actions of another via electronic communications or observing or spying on another resulting in real fear in his thoughts, or taking a photograph or recording a video without his consent in a manner that harms that person's reputation.
5. *Pornography:* People or organizations participating in the child sex business become extremely wealthy in a quite short period of time. Sexual exploitation of little girls is a lucrative industry for such evil and horrible adults. Ukraine is regarded as a major market for child pornography. It is even manufactured in huge quantities there.
6. *Electronic Fraud:* Anyone who misuses an information system or data with the objective of causing harm or destruction to the public or another person, or who makes an unauthorized claim or title to some property, or who enters into an agreement to conduct fraud, shall face three years in jail or a fine of two LACS and fifty thousand rupees, or both.
7. *Virus Attacks:* Two brothers from Sialkot pioneered this idea and built this computer software with noble intentions, the goal being to eliminate piracy. 'Brains' was the title given to the first virus that they created. The goal of this programme was to limit and prevent the creation of pirated and duplicated original software. However, as time and technology progressed, this application was also employed for nefarious reasons. Viruses are little software programmes designed to spread from one computer to another and disrupt computer systems and activities.
8. *Impersonation:* To try to fool someone by appearing to be someone else. It is both unlawful and unethical to do so. Such activities are committed to slander a person, corporation, or other entity by disseminating false and inaccurate information, explicit content, and so on. This is a type of identity theft.

Today is the era of data, and in a decade's time, it will be the period of data currency. However, technological advancement is directly proportionate to cybercrime. Because a new programme is created every day, as well as a new approach to break that specific conduct, the diversified form of cybercrime makes inquiry tough for different organizations. Technological growth is becoming more sophisticated, and because cybercrime and technology are inextricably linked, there is still a long way to go. As technology advances, a new method of interfering with and hacking into it is developed.

Nations such as China, the United States of America, England, France, Japan, Korea, and others are regarded as the top digital and information technology centers, however owing to cyber-criminal activities, the aforementioned countries have faced major problems and loss amounting to billions of dollars. Any organization or corporation cannot create a proper system or software that can deal with

all cyber criminals and their cybercriminal activities. Is it possible to eradicate cybercrime? The answer is "no," and it can only be limited to a certain amount.

Online stalking, cyber harassment, spoofing, spamming, extortion, abduction, and terrorism are all major issues in Pakistan. The government passed the "Prevention of Electronic Crime Act" in 2016 [23]. It was extremely beneficial to the Federal Investigation Agency (FIA). However, there are still several faults. The problem persists in the absence of a cybercrime policy, adequate investigation methodologies, and professionals in computer and digital forensics. It is unavoidable that academia, specialists, and the military will play a role in countering cybercrime. However, a balance must be struck between cyber security and citizens' basic rights. If the former infringes on the latter, it will fail. Such issues must be addressed on an emergency basis.

Overcoming such issues is not a tough endeavor. The digital world is growing at a breakneck pace. All of the industrialized nations' contemporary economies, education systems, and so on are founded on information technology and advanced digital systems. Pakistan is still developing and catching up with the rest of the globe. They are a decade ahead of us due to their technology. To compete with the contemporary developed world, we must prioritize our IT industry. The government must establish a faultless policy on cybercrime, the digital world, and information technology so that we can compete with first-world countries.

3 Background

Due to the failure of traditional cybercrime detection approaches, the number of cybercrimes increases at a very high rate. Cybercriminals adopt new technologies and improve their methods to achieve their illegal goals. Numerous methods have been developed to detect cybercrimes. These include statistical, machine learning, neural networks, deep learning, data mining, computer vision, biometric and forensics tools. The Hidden Markov Model (HMM) is although termed as one of the best approaches to detect cyber-attacks, but a time-consuming process. Using N-gram extraction algorithm, the improved version of HMM was proposed [24]. A system based on Bayesian learning network was developed for detecting cybercrimes network [25]. Bayesian network uses probabilistic models which is more suitable for noisy environments. However, the model compromises in real environments. Machine learning approaches are widely used in cybercrime detection. Decision tree is one of the basic learning models used to achieve high detection accuracy [26]. Levenshtein algorithm, naïve Bayes, JRip, J48, and support vector machine (SVM) classifier have been used to predict cyberbullying [27–29].

To detect phishing emails, a hybrid features tool consists of machine learning, feature vector generation, method selection and feature evaluation was proposed to extract feature vectors [30]. A multilayer feed forward neural network is also used to detect phishing attacks [31]. A comparison of K-Nearest Neighbour (KNN), decision tree and random forest algorithms were carried out in detecting the cybercrimes [32]. Random forest outperforms the other two classification algorithms. Visualization techniques are utilized to detect malware in smartphones with Android platform [33]. A K-means clustering is used to detect crime patterns in different geographical regions [34]. Embedded programming, software engineering, agent-based methods, and artificial intelligence approaches [35] have been widely used to detect the cyber-attacks. The IP addresses are used to determine the user location and detect the real-time cyber-attack. A cybercrimes detection system was proposed based on data mining called Apriori algorithm [36]. To identify association between crimes, a framework was implemented for the general crimes instead of cybercrimes [37]. The aim was to establish a data

mining approach to accurately categorize the crimes including cybercrimes. In general, data mining has the capability to explore large amount of data in efficient and speedy manner.

Association Rule Mining (ARM) is one of the data mining approaches that have been widely used in crime research [38]. Association rules extracts relevant criminal evidence from a large set of crime data, find patterns of interest and connection between different crimes. Law enforcement agencies can be benefited during crime investigation and prevention. An incremental algorithm [39] was proposed to discover the crime patterns in Hong Kong using the time series data consist of time expressions. To discover the latest and serious nature crimes, the application of the FP-growth algorithm was analyzed [40] to bring improvements in crime detection. Fuzzy association rule mining was applied to explore the community crime patterns to reduce the crime rate [41]. A number of algorithms such as Apriori algorithm, FP-growth algorithm, and FP-Tree similarity algorithm were tested and concluded that each algorithm has their own pros and cons [42]. ARM has been extensively used to analyze a criminal dataset quantitatively and extract comprehensive rules used for crime prevention [43]. A crime mapping model based on geographic and demographic information using association rule mining was employed to monitor the crime occurrence at a specific area [44]. The model demonstrates good results and was highly recommended to be used in analyzing future crime hot spots to prevent crimes incidents. The performance of ARM in crime investigation has been acknowledged worldwide [45] and numerous flavors of ARM-based algorithms have been developed for criminal forensic analysis, suspect analysis, and behavior analysis [46].

4 Methodology

Ant Colony Optimization (ACO) algorithm [47] is a Swarm Intelligence algorithm that has been inspired by real ants. Ants are almost blind and live in colonies. They use a chemical for mutual communication while searching for food. Each ant deposits some amount of pheromone on its path for guidance of other ants. Initially, ants move randomly. With the passage of time, when one or more ants successfully find a shortest path from nest to food source, pheromone amount increases on the path which guides other ants to this path. Pheromone on least recently-used paths is evaporated over time, hence level of misguidance is reduced and eventually, all ants converge to the same path which is either shortest or near-shortest. Artificial ants use the idea of pheromone for communication. In addition to that, a problem-dependent heuristic function is used along with pheromone to calculate selection probability of data items for discovery of patterns or rules. For instance, searching for a shortest path between to nodes in a network, reciprocals of their mutual distance is a very good choice for heuristic. It is important to note that ACO is used for discrete datasets which allows its structure to be mapped to a finite set of states (nodes) and/or links between nodes.

The proposed study utilizes the Ant Colony Optimization (ACO) for associative classification to map patterns in the underlying dataset tor the class (Crime Type). A *term* in the ACO-based Associative Classification refers to name of a feature and one of the feature's possible discrete values, i.e., $X = v1$ is a terrn which refers to value $v1$ of feature X. The Ant Colony Optimization algorithm is represented using the graph data structure. Fig. 5 represents a sample representation of ACO graph. Each node in the graph represents a feature term of the provided data. Each edge represents the strength of association between the two nodes it connects. The strength of association is directly dependent on the problem-dependent heuristic value for that connection (edge).

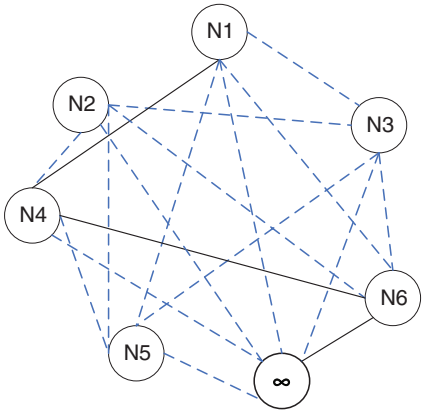


Figure 5: Ant Colony Optimization algorithm as graph data structure

The graph in Fig. 5 consists of 7 nodes. Let us assume that there are three features (attributes) of the given dataset each having two distinct values. Nodes N1 and N2 belong to one attribute (i.e., N1 and N2 are two possible values of a specific attribute, one of which can be present in a data instance), nodes N3 and N4 denote attributes of 2nd attribute while N5 and N6 represent distinct values of third attribute. Since N1 and N2 are terms (distinct values) of the same attribute (feature), therefore they are not mutually connected. This is because when an ant would choose N1, N2 would not be selected by that ant. The same is the case with other nodes.

All the terms of a feature are mutually exclusive and hence have no mutual links. The node labeled with ∞ represents the "sink" node. When the sink node is selected, search terminated and the rule class is determined and rule quality is calculated. The dashed lines in the figure represent the possible terrains for search in the search space, while solid lines represent a sample search path taken by an ant. The rule classification rule antecedent for the sample ant search yields *if N1 AND N4 AND N6*. The rule consequent (the class label) may be chosen based on the frequency of the antecedent in all classes. The class containing the highest frequency of the discovered antecedent will be assigned as the rule consequent.

Fig. 6 demonstrates the flowchart of the Ant Colony Optimization algorithm used for Associative Classification. The first step is to discretize the input dataset. In this step if any feature contains numerical continuous values, they are converted to some discrete values because the ACO operated only on discrete data. In the next step, the outlier values are removed followed by reading the dataset into training and test sets. In the following step, the pheromone and heuristic values are initialized. The rule collection is then initialized. Since the ACO algorithm used for associative classification uses "Select Class First" approach, therefore, the rules for each class are constructed selecting one class after another.

The index represents the class index of the selected class. Initially it is set to 1 to select the first class. The class selection process continues until the class index exceeds the number of classes in the dataset. Variable NC represents the number of dataset classes. If the (class) Index variable exceeds NC the algorithm stops rule construction and sorts rules. Otherwise, rules for each class C are constructed. First, single-term (non-associative) rules are constructed using each term for class C. If any of the single-term rules has support and confidence meeting the minimum support and confidence (parameter) threshold values, that rule is added to the class rule list. After construction of sing-term rules, each ant is used to construct multi-term (associative) rules. The same criterion for retaining

of the single-term rules is applied also for the rules constructed by ants. Pheromone and selection probabilities are updated according to the rule confidence.

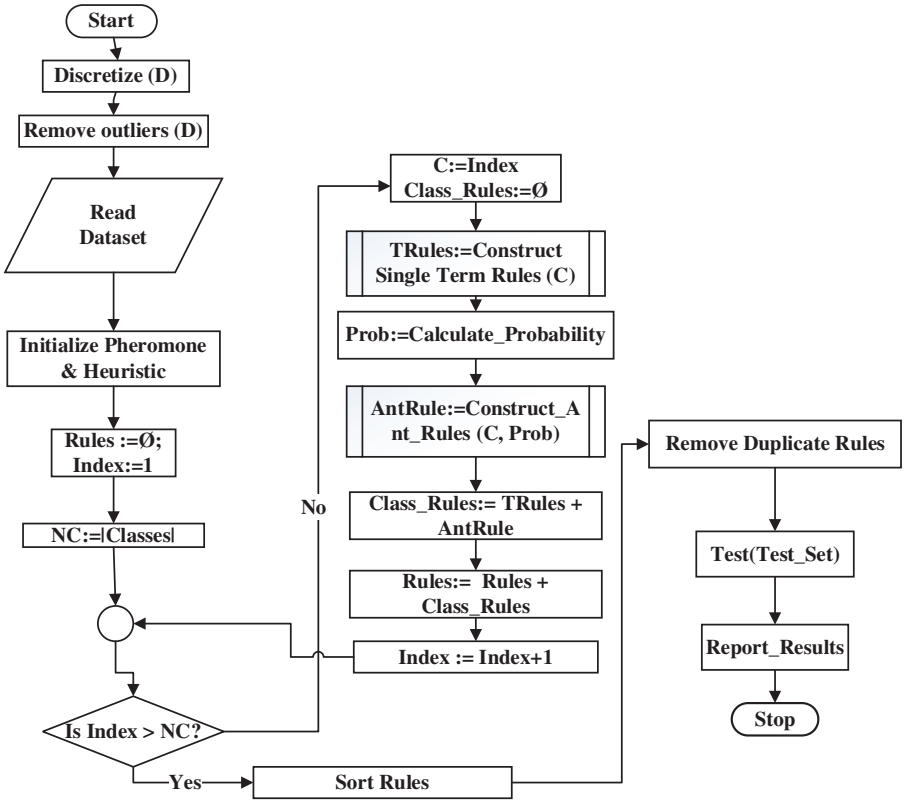


Figure 6: A flowchart of the Ant Colony Optimization (ACO) algorithm used for associative classification

It is very important that if a single-term rule does not meet the minimum support and minimum confidence criteria defined by the user/programmer, its pheromone and selection probability values are set to 0 because single-term rules drive the probability of association among multiple terms. When all ants complete rule construction, class rules are added to the final rule list and Index is incremented to point to next class. When rules for all classes are constructed, the final rule list is sorted in the descending order of confidence and support. Duplicate rules (if any) are removed in the next step. Finally, the rule list is evaluated on the test set to calculate rule accuracy and results are reported to the user.

Algorithm 1 lists down steps of the proposed computational methodology. The given data set is divided in to *TrainingSet* and *TestSet*. ACO-based associative classification algorithm learns on *TrainingSet* while its results are evaluated on *TestSet*.

ACO consists of two major ingredients, i.e., a problem-dependent *Heuristic* function and *Pheromone*. Heuristic remains constant throughout the execution of the algorithm. This is calculated in the first step. Heuristic value for each term *i i*s calculated according to the Eq. (1).

$$\eta_i = \frac{|term_i, class_k| + 1}{|term_i| + |Classes|} \tag{1}$$

where η_i represents the heuristic value for ith term when the term is the first term, to be selected by an ant. Class (k) refers to the kth class (crime type). For each subsequent term j, the Eq. (2) is used to calculate heuristic:

$$\eta_{ij} = \frac{\left|term_i, term_j, class_k\right| \times |term_j, class_k|}{|term_i, class_k| \times |Class_k|} \tag{2}$$

Step 2 initializes ACO and associative classification parameters. ACO parameters include number of ants (n) and pheromone evaporation rate ρ. Number of ants is usually kept between 10 and 100 while pheromone evaporation rate is in range (0, 1). Since pheromone guides the search process, its evaporation assists in "forgetting" undesired or infeasible paths. Associative classification takes two parameters, i.e., minimum support (*minSupp*) and minimum confidence (*minConf*). Minimum support is the threshold of the ratio of frequency of a pattern in the dataset to be considered as an associative rule, while minimum confidence is the ratio of frequency of the discovered pattern with a particular class. Usual values of minimum support and minimum confidence are in ranges (0, 0.3) and (0, 0.6), respectively.

Step 4 initializes the pheromone trails for guidance of ants. It is a 2-dimension square matrix of size equal to number of terms in the dataset. Pheromone value for each term i to term j s given by the Eq. (3).

$$\tau_{ij} = \frac{1}{|Terms|} \tag{3}$$

where represents pheromone value of term j from term i while $|Terms|$ represents the number of terms in the dataset. Step 5 initializes the global rule list to an empty set. This list contains all the rules constructed during the training. Steps 7 to 20 are repeated for each class. Step 8 is used to construct 1-term rules for each term mapping to class c. The rules that meet minimum support and minimum confidence threshold are retained and added to class rules (step 9).

Step 10 is used to initialize selection probabilities of terms. These probabilities guide the selection of terms of rules. Steps 13 to 18 are repeated to construct rules of length g which varies from 2 to number of attributes (step 12). Steps 14 to 16 describe the procedure of rule construction by ants. Each ant t constructs a rule consisting of at most g number of terms (step 15). If support and confidence of the constructed rule are greater than or equal to minimum support and minimum confidence thresholds receptively, the rule is appended to the multi-term rule list (step 16).

Algorithm 1: ACO-based associative classification

1. Calculate Heuristic
2. Initialize parameters
3. Initialize terms
4. Initialize Pheromone
5. Set $RuleList = \varnothing$
6. Repeat steps 7–20 for each class c
7. Set $ClassRule = \varnothing$
8. Scan *TrainingSet* to construct 1-term rule *TRules* for each term and class c
9. Append *TRules* to *ClassRules*
10. Calculate selection probability of each term
11. Set $Ruleg = 2$
12. Repeat steps 13–18 until $g = [Attributes]$

(Continued)

Algorithm 1 (continued)

13. Set $MTRules = \varnothing$
14. Repeat steps 15–16 for each ant t
15. Let and t construct a rule R containing at most g (randomly-selected) terms guided by selection probability of each term.
16. If $Support\,(R) \geq minSupp\,and\,Confidence\,(R) \geq minConf$ then add R to $MTRules$
17. Update pheromone and selection probability.
18. Set $g = g + 1$
19. Append $MTRules$ to $ClassRules$
20. Append $ClassRules$ to $RuleLis$
21. Sort $RuleList$ in descending order of $Confidence$ and $Support$
22. Test $RuleList$ on $TestSet$
23. Display Results

Step 17 is used to update the pheromone according to the following pair of equations. The first equation is used to evaporate the pheromone values of all trails (decreased), while the latter is used to update (increase) the pheromone values of terms used in the discovered rules that meet the criteria of minimum support and confidence according to their support and confidence. Eq. (4) is for Pheromone evaporation.

$$\tau_{ij}\,(g)' = \tau_{ij}\,(g) \times (1 - \rho) \tag{4}$$

where $\tau_{ij}\,(g)$ represents the pheromone value at the link between term I and term j in generation (or iteration) g, $\tau_{ij}\,(g)'$ denotes the value of the pheromone after evaporation, while ρ represents the pheromone evaporation rate. The Pheromone value of term i to term j is given by Eq. (5).

$$\tau_{ij}\,(g+1) = \tau_{ij}\,(g)' + \tau_{ij}\,(g)' \times \left(1 - \frac{1}{1 + conf_r}\right) \tag{5}$$

where $conf_r$ denotes the confidence of the rule r in which the terms i and j are part of the antecedent.

Step 19 is used to add the ant-constructed rules to the list of class c rules. Step 20 adds rules of class c to the global rule list and hence the procedure for rule construction for class c concludes. This process is repeated for every class. Step 21 sorts the rule list in descending order of confidence and support. In step 22, the rule list is evaluated for performance on test set. Results of the performance are displayed in step 23. The algorithm can be utilized in K-fold cross-validation to get a fine-grained and generalized study of results. The sample data and examples for calculating pheromone and heuristic values can be found in [48].

5 Dataset

The data used for this work is provided by the Federal Investigation Agency (FIA), Government of Pakistan. The data provided before preprocessing include the Reporting Center Name, District, Gender, Year, Profession, Offence, Complaint Received via, Complaint Received From, Crime Type, and Medium Used for the crime. Three of the attributes namely Reporting Center, Name, and Year are excluded from the dataset. Crime type samples with more than 1500 instances are picked up for training and testing. The remaining dataset consist of total 116520 instances.

Table 1 represents the refined crime dataset used for analysis consists of 7 (non-class) attributes and 16 classes (Crime Type as class label). There are sixteen classes of data used for classifier

evaluation. These classes are crime types specified in the input data. Table 2 lists the names and frequencies of classes.

Table 1: Data description

S. No.	Attribute name	No. of distinct values
1	District	11
2	Gender	2
3	Profession	20
4	Offence	25
5	Received via	4
6	Received from	5
7	Medium used	26

Table 2: Class distribution

S. No.	Class label	Frequency
1	Anti-Army	2480
2	Anti-Religion	4000
3	Blackmailing	7620
4	Blasphemous-Contents	3940
5	Defamation	7000
6	Fake-Profile	7280
7	Financial-Frauds	26460
8	Hacking	13000
9	Harassment	15020
10	Identity-Theft	1600
11	Invalid-Complaint	6140
12	Irrelevant-Complaint	9200
13	Online-Job-Frauds	2060
14	Online-Shopping	2800
15	Threats	3360
16	Un-Authorized-Access	4560
	Total	116520

6 Results and Discussions

The AC-ACO is of parametrized algorithm which needs specific values for its parameters to run properly. The parameters include number of ants, folds, minimum coverage, minimum support, minimum confidence and pheromone rate. The details are given in Table 3. Parameter values have been

taken from [48] and have been modified experimentally, e.g., Minimum Confidence has been changed from 0.45 to 0.20 fir better results.

Table 3: Parameter specifications

S. No.	Parameter name	Value
1	No. of ants	15
2	No. of folds	10
3	Minimum coverage	1.0
4	Minimum support	0.03
5	Minimum confidence	0.20
6	Pheromone evaporation rate	0.09

The classifier was evaluated on the given dataset for discovery of associative classification rules with 10 cross-fold validation mechanism. In this mechanism, 90% of the data is used for training and 10% is used for testing the classifier. This process is repeated 10 times, each time instances are varied in training and test sets to keep the classifier diverse. Table 4 lists the output values of the result of a sample run, and True Positive and True Negative rates for each class are shown in Table 5.

Table 4: Evaluation results

Measure	Value
Accuracy	95.23%
Precision	0.97
Recall	0.89
F-Measure	0.93

Table 5: True positive rates (TPR) and true negative rates (TNR)

S. No.	Class label	Frequency	Accuracy	Precision	Recall (TPR)	TNR	F-Measure
1	Anti-Army	2480	87%	1.00	0.87	1.00	0.93
2	Anti-Religion	4000	100%	1.00	1.00	1.00	1.00
3	Blackmailing	7620	94%	1.00	0.94	1.00	0.97
4	Blasphemous-Contents	3940	81%	1.00	0.81	1.00	0.89
5	Defamation	7000	95%	1.00	0.95	1.00	0.98
6	Fake-Profile	7280	96%	1.00	0.96	1.00	0.98
7	Financial-Frauds	26460	100%	1.00	1.00	1.00	1.00
8	Hacking	13000	100%	1.00	1.00	1.00	1.00
9	Harassment	15020	100%	1.00	1.00	1.00	1.00
10	Identity-Theft	1600	59%	1.00	0.59	1.00	0.74
11	Invalid-Complaint	6140	100%	1.00	1.00	1.00	1.00
12	Irrelevant-Complaint	9200	100%	1.00	1.00	1.00	1.00
13	Online-Job-Frauds	2060	84%	1.00	0.84	1.00	0.92
14	Online-Shopping	2800	78%	1.00	0.78	1.00	0.88
15	Threats	3360	51%	1.00	0.51	1.00	0.68

(Continued)

Table 5 (continued)

S. No.	Class label	Frequency	Accuracy	Precision	Recall (TPR)	TNR	F-Measure
16	Un-Authorized-Access	4560	100%	0.45	1.00	0.95	0.62
	Total	**116520**	**95.23%**	**0.9528**	**0.9533**	**0.9969**	**0.9530**

Table 5 lists down class-wise accuracies achieved by AC-ACO. The proposed algorithm showed more than 90% accuracy on half of the classes. AC-ACO showed 100% accuracy to predict 7 out of 16 classes. Overall accuracy achieved by AC-ACO was 95.23%. The algorithm showed poor performance to predict two classes *Threats* (51% accuracy) and *Identity-Theft* (59% accuracy). The Identity-theft class has the lowest frequency in the dataset (approximately 1.37%) while the Threats class has about 2.83% instances in the entire dataset. Although Online-Shopping has lower frequency but AC-ACO showed a much better accuracy of 78% to predict instances of this class. Precision for 15 classes is 1 because false positive (FP) values for these classes were 0. However, FP rate for the Threat class has been higher due to false negative prediction of all other classes were erroneously predicted to this class. Hence, FP rate of the Threat class was very high. The impact of FP rate is visible on TP rate and accuracy for each class.

Maximizing the classification accuracy is the prime goal of a classifier. It is the percentage of instances from the test set that are correctly classified by the classifier. Precision and recall measures demonstrate the ability of the classifier to distinguish the target class labels from other class labels. F-measure is simply the harmonic mean of precision and recall measures and the goal of the classifier is to maximize this value too. A high F-Measure score (closer to 1) indicates that the classifier accuracy is not merely just because of a dominant majority class.

The ACO-based associative classification model applied in this study showed F score of 0.97 which is almost the same as the accuracy. This implies that the achieved accuracy is not merely due to frequency of classes. Table 6 represents the overall ranking trends of top five medium used in cybercrimes and the top five offences in Pakistan after applying the association rules using the ACO algorithm. Table 7 lists top 20 rules of a fold of a sample run of the ACO-assisted associative classification model used for discovering associativity among features as between feature-space and class labels in the given dataset.

Table 6: Top five medium used in cybercrimes

Rank	Medium	Offence
1	Phone call	Electronic fraud
2	EasyPaisa	Unauthorized access
3	Email	Hate speech
4	Olx	Tempering
5	YouTube	Glorification

Table 7: Sample rules list

Rule	Attributes	Class	Conf.	Supp.
1	Medium-Used=EasyPaisa	Financial-Frauds	1.00	0.14
2	Offence=Unauthorized-ID-Info And Medium-Used=Email	Anti-Army	1.00	0.08
3	District=Bahawalpur And Medium-Used=Email	Anti-Army	1.00	0.02
4	Offence=Cyber-terrorism And Medium-Used=Phone-Call	Threats	1.00	0.02
5	Offence=Cyber-terrorism And Medium-Used=Email	Anti-Army	1.00	0.02
6	Gender=Male And Offence=Offences-DignNP And Medium-Used=YouTube	Defamation	1.00	0.01
7	Offence=Interference-Crit-Info-Sys And Medium-Used=Others	Identity-Theft	1.00	0.01
8	Gender=Male And Offence=Unauthorized-Copy-Tr And Medium-Used=Others	Identity-Theft	1.00	0.01
9	Gender=Male And Offence=Others-Cybercrime And Received-From=Individual And Medium-Used=Olx	Identity-Theft	1.00	0.01
10	District=Bahawalpur And Offence=Unauthorized-ID-Info And Received-via=Online-Form And Medium-Used=Others	Identity-Theft	1.00	0.01
11	District=Faisalabad And Offence=Unauthorized-ID-Info And Received-From=Individual And Medium-Used=Others	Identity-Theft	1.00	0.01
12	Medium-Used=JazzCash	Financial-Frauds	0.99	0.12
13	Medium-Used=ATM-Card	Financial-Frauds	0.96	0.02
14	Gender=Male And Offence=Already-Exist And Medium-Used=Email	Anti-Army	0.94	0.13
15	Medium-Used=IBFT	Financial-Frauds	0.94	0.02
16	Medium-Used=Online-Banking	Financial-Frauds	0.92	0.04
17	District=Islamabad And Offence=Invalid-Complaint And Received-via=Online-Form And Medium-Used=Facebook	Fake-Profile	0.91	0.11
18	Medium-Used=Olx	Financial-Frauds	0.88	0.08
19	District=Faisalabad And Offence=Offences-DignNP	Defamation	0.88	0.02

(Continued)

Table 7 (continued)

Rule	Attributes	Class	Conf.	Supp.
20	District=Islamabad And Offence=Already-Exist And Medium-Used=Email	Anti-Army	0.81	0.14

The listed rules are sorted by confidence in descending order. More confident rules tend to provide more accurate results. Six associative classification rules have confidence value of 1 (100%).

Rule 1 states that in 14% of instances of financial fraud, Easy-Paisa (a money-transfer service) was used as a medium with 100% confidence. The 100% confidence means that all such instances in which Easy-Paisa was used as a medium were financial fraud type of crime.

According to rule 2, 8% crime instances in the training dataset observer "Unauthorized ID info" offence through email. This pattern very strongly belongs to the crime type "Ant-Army" (with 100% confidence). In general, there are 11 rules whose confidence is 100% with at least 1% support.

The graphical representation of rules support and confidence values for each of the rules listed in Table 7 is presented in Fig. 7.

Figure 7: Graphical representation of rule support and confidence

The performance of the AC-ACO was compared with performance of Ant Miner [21] and Random Forest (RF) [22] algorithms. All three algorithms were evaluated on 10 cross-fold validation to avoid any biased results. AC-Common parameters for Ant Miner and AC-ACO were kept equal.

Table 8 illustrates the performance comparison of AC-ACO with Ant Miner and Random Forest algorithms.

Fig. 8 displays the comparison of performance of AC-ACO with its competitors visually. The results shown above demonstrate that the proposed AC-ACO algorithm quite comprehensively outperformed its competitors with respect to accuracy, precision, recall and F-measure statistics. Although Random Forest (RF) algorithm works on information gain measure for classification, but since it is a greedy search technique which fails in finding generalized mapping between the feature set and class labels. RF showed 65.70% accuracy on the underlying dataset. The Ant Miner algorithm is an ACO-based classifier but it does not incorporate mutual association among features in the underlying

dataset, therefore it also showed poor performance. The classification accuracy achieved by Ant Miner for the underlying crime reports dataset was 61.4%.

Table 8: Performance comparison of AC-ACO with its competitors

Algorithm	Accuracy	Precision	Recall	F-Measure
Ant miner	0.6142	0.5911	0.6104	0.5614
Random forest	0.6570	0.6320	0.6570	0.6220
AC-ACO	**0.9523**	**0.9658**	**0.8898**	**0.9263**

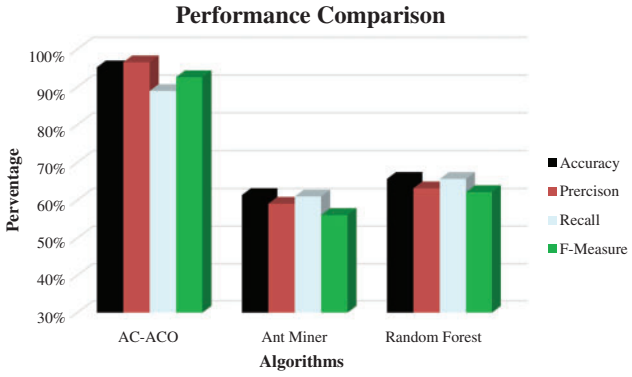


Figure 8: Performance comparison of AC-ACO, ant miner and random forest algorithms

Analyzing the above results demonstrate that Associative Classification using Ant Colony Optimization (AC-ACO) performed much better than its competitors and showed 95% accuracy. It also highlighted potential associativity among features of the dataset.

7 Conclusions

Associative Classification based on Ant Colony Optimization (AC-ACO) has been applied to identify association among activities performed while commuting crimes. AC-ACO discovers frequent patterns of criminal activities and maps such patterns to crime types. The proposed model utilizes the diversity and optimal search capabilities of ACO and robustness of associative classification to build an accurate and robust classifier. The algorithm was applied on the crime data provided by the Federal Investigation Agency (FIA), Government of Pakistan. The dataset consists of more than 110 thousand instances and 16 crime types. The performance of AC-ACO was compared with Random Forest and Ant Miner algorithms. The experimental results based on 10 cross-fold validation showed that AC-ACO comprehensively outperformed both of its competitors in accuracy. Statistical measures prove that the high performance shown by AC-ACO was not by chance but the discovery of associative classification rules enabled the algorithm to achieve a very high overall classification accuracy of 95%. As a future direction, it is recommended to perform an empirical study of parameters for fine-tuning of associative parameters *min support* and *min confidence*.

Acknowledgement: The authors would like to thank the Federal Investigation Agency (FIA), Government of Pakistan for providing the data, valuable knowledge and their support in completing this research work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Tsakalidis and K. Vergidis, "A systematic approach toward description and classification of cybercrime incidents," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 4, pp. 710–729, 2019.
[2] A. Unwala, "Snowden and U.S. cyber power," *Georgetown Journal of International Affair*, vol. 4, no. 1, pp. 4–11, 2014.
[3] E. Schmidt and J. Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*. London, UK: John Murray, 2014.
[4] R. C. Maness and B. Valeriano, "The impact of cyber conflict on international interactions," *Armed Forces and Society*, vol. 42, no. 2, pp. 301–323, 2016.
[5] A. Kosenkov, "Cyber conflicts as a new global threat," *Future Internet*, vol. 8, no. 3, pp. 45, 2016.
[6] M. Yar and K. F. Steinmetz, *Cybercrime and Society*. Newbury Park, CA, USA: Sage, 2019.
[7] M. R. Alahmad and I. I. Hashem, "A comprehensive study on cyber terrorism: Concept, effects, and prevention," *Journal of Information Privacy and Security*, vol. 17, no. 2, pp. 116–127, 2021.
[8] "The Morris Worm," 2018. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218
[9] E. Mousavinejad, F. Yang, Q. L. Han and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 11, pp. 3254–3264, 2018.
[10] C. Wu, Z. Hu, J. Liu and L. Wu, "Secure estimation for cyber-physical systems via sliding mode," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3420–3431, 2018.
[11] T. Czosseck, K. Stavrou and M. Meinel, "Cyber warfare: A new challenge for international law," *Journal of Conflict & Security Law*, vol. 26, no. 1, pp. 123–146, 2021.
[12] "ICS alert (IR-ALERT-H-16-056-01): Cyber-attack against Ukrainian critical infrastructure," 2016. https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01
[13] K. J. Higgins, "Lessons from the Ukraine electric grid hack," 2016. https://www.darkreading.com/vulnerabilities-threats/lessons-from-the-ukraine-electric-grid-hack
[14] E. V. S. Farhana, "Cyber crimes and the victimisation of women," *International Journal of Law Management & Humanities*, vol. 5, no. 1, pp. 1877, 2022.
[15] A. N. Shaikh, A. M. Shabut and M. A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," in *Proc. of the 10th Int. Conf. on Software, Knowledge, Information Management and Applications (SKIMA)*, Chengdu, China, pp. 9–15, 2016.
[16] S. S. Chakkaravarthy, D. Sangeetha, M. Venkata Rathnam, K. Srinithi and V. Vaidehi, "Futuristic cyber-attacks," *International Journal of Knowledge-Based and Intelligent Engineering Systems*, vol. 22, no. 3, pp. 195–204, 2018.
[17] "SQL Injection," 2022. https://portswigger.net/web-security/sql-injection
[18] R. Gohil and A. Patel, "Survey on network security threats, solutions and technologies," *Journal of Network and Computer Applications*, vol. 149, pp. 142–457, 2020.
[19] A. Tabasum, Z. Safi, W. AlKhater and A. Shikfa, "Cybersecurity issues in implanted medical devices," in *Proc. of the Int. Conf. on Computing Applications*, Beirut, Lebanon, pp. 1–9, 2018.
[20] R. Coulter, Q. L. Han, L. Pan, J. Zhang and Y. Xiang, "Data-driven cyber security in perspective-intelligent traffic analysis," *IEEE Transactions on Cybernetics*, vol. 50, no. 7, pp. 3081–3093, 2020.
[21] U. Ayub, H. Naveed and W. Shahzad, "PRRAT_AM—An advanced ant-miner to extract accurate and comprehensible classification rules," *Applied Soft Computing*, vol. 92, no. 16, pp. 106326, 2020.
[22] Y. Lin and X. Wang, "A data-driven scheme based on sparse projection oblique randomer forests for real-time dynamic security assessment," *IEEE Access*, vol. 10, pp. 79469–79479, 2022.

[23] Prevention of Electronic Crimes Act (PECA), 2016. https://na.gov.pk/uploads/documents/1470910659_707.pdf
[24] X. Yang and X. Li, "Improved hidden Markov model with common frequent patterns for intrusion detection in IoT," *Security and Communication Networks*, vol. 2020, no. 7, pp. 1–10, 2020.
[25] M. J. Durst and M. J. Scrofani, "A Bayesian network model for detecting financial cybercrimes," *Journal of Financial Crime*, vol. 26, no. 4, pp. 1108–1124, 2019.
[26] R. Kumar and A. Bhat, "A study of machine learning-based models for detection, control, and mitigation of cyberbullying in online social media," *International Journal of Information Security*, vol. 21, no. 6, pp. 1409–1431, 2022.
[27] B. S. Nandhini and J. I. Sheeba, "Cyberbullying detection and classification using information retrieval algorithm," in *Proc. of the Int. Conf. on Advanced Research in Computer Science, Engineering and Technology (ICARCSET) ICARCSET*, Unnao, India, pp. 20, 2015.
[28] J. Batani, E. Mbunge, B. Muchemwa, G. Gaobotse, C. Gurajena *et al.,* "A review of deep learning models for detecting cyberbullying on social media networks," in *Cybernetics Perspectives in Systems: Proc. of 11th Computer Science On-Line Conf. 2022*, Putrajaya, Malaysia, vol. 3, pp. 528–550, 2022.
[29] M. A. Al-garadi, K. D. Varathan and S. D. Ravana, "Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network," *Computers in Human Behavior*, vol. 63, no. 1, pp. 433–443, 2016.
[30] S. D. Guptta, K. T. Shahriar, H. Alqahtani, D. Alsalman and I. H. Sarker, "Modeling hybrid feature-based phishing websites detection using machine learning techniques," *Annals of Data Science*, vol. 2, no. 3, pp. 1–26, 2022.
[31] C. Catal, G. Giray, B. Tekinerdogan, S. Kumar and S. Shukla, "Applications of deep learning for phishing detection: A systematic literature review," *Knowledge and Information Systems*, vol. 64, no. 6, pp. 1457–1500, 2022.
[32] H. Daumé III, "A course in machine learning," vol. 5, 2012. http://ciml.info/
[33] F. M. Darus, N. A. A. Salleh and A. F. M. Ariffin, "Android malware detection using machine learning on image patterns," in *Proc. of the Cyber Resilience Conf. (CRC)*, Putrajaya, Malaysia, pp. 1–2, 2018.
[34] S. V. Nath, "Crime pattern detection using data mining," in *Proc. of the IEEE/WIC/ACM Int. Conf. on Web Intelligence and Intelligent Agent Technology*, Hong Kong, China, pp. 41–44, 2006.
[35] J. Raiyn, "A survey of cyber attack detection strategies," *International Journal of Security and its Applications*, vol. 8, no. 1, pp. 247–256, 2014.
[36] F. Mustafa and N. S. Raja, "Analysis of digital forensics in cybercrime investigation using data mining techniques," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 2, pp. 184–189, 2020.
[37] S. S. Jadhav and P. N. Pawar, "Crime analysis and prediction using machine learning techniques," *Procedia Computer Science*, vol. 165, pp. 63–70, 2019.
[38] B. Shannaq, "Machine learning model-ensuring electronic exam quality using mining association rules," *Machine Learning*, vol. 29, no. 3, pp. 12136–12146, 2020.
[39] V. Ng, S. Chan, D. Lau and C. M. Ying, "Incremental mining for temporal association rules for crime pattern discoveries," in *Proc. of the 8th Aust. Database Conf.*, Victoria, Australia, pp. 123–132, 2007.
[40] Y. Tan, Z. Qi and J. Wang, "Applications of association rules in computer crime forensics," *Applied Mechanics and Materials*, vol. 157–158, pp. 1281–1286, 2012.
[41] Z. Zhang, J. Huang, J. Hao, J. Gong and H. Chen, "Extracting relations of crime rates through fuzzy association rules mining," *Applied Intelligence*, vol. 50, no. 2, pp. 448–467, 2020.
[42] D. Usha and K. Ramesh Kumar, "A complete survey on application of frequent pattern mining and association rule mining on crime pattern mining," *International Journal of Advanced Computer Science and Technology*, vol. 3, pp. 264–275, 2014.
[43] L. Wang and B. Sun, "Analysis of public security case base based on data mining," *GAN Science and Technology*, vol. 12, no. 3, pp. 18–22, 2018.

[44] S. A. Asmai, N. Izzatul, A. Roslin, R. W. Abdullah and S. Ahmad, "Predictive crime mapping model using association rule mining for crime analysis," *Science International*, vol. 26, pp. 1703–1706, 2014.
[45] N. Al Mutawa, J. Bryce, V. N. Franqueira, A. Marrington and J. C. Read, "Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes," *Digital Investigation*, vol. 28, no. 12, pp. 70–82, 2019.
[46] N. Yu, *Research on the Discovery Method of Suspicion Degree Relationship Based on the Association Rule Algorithm*. Dalian: Dalian Polytechnic University, 2015.
[47] M. R. Kounte, E. Niveditha, K. Afrose and A. S. Sudeshna, "Problem solving techniques using ant colony optimization in computational intelligence," in *ICDSMLA 2020: Proc. of the 2nd Int. Conf. on Data Science, Machine Learning and Applications*, Singapore, pp. 739–747, 2022.
[48] H. H. Awan and W. Shahzad, "Semi-supervised associative classification using ant colony optimization algorithm," *PeerJ Computer Science*, vol. 7, no. 4, pp. e676, 2021.