A SYSTEMATIC APPROACH TOWARDS CLASSIFICATION AND DESCRIPTION OF CYBER CRIME INCIDENTS

Dulam Bhavya Sree
MTech,
Department of Computer Science
Cambridge Institute of Technology
Bangalore, Karnataka

K. Satyanarayan Reddy
Professor & HOD
Department of Information Science and Engineering
Cambridge Institute of Technology, Affiliated to VTU
Bangalore, Karnataka

***Abstract*—** This paper reviews the classification of Cybercrime Incidents. This work offers a comprehensive considerate of cybercrime incidents and their corresponding offences combining a series of approaches reported in relevant literature. Initially, this work reviews and identifies the features of cybercrime incidents, their respective elements and proposes a combinatorial incident description schema. These offences are well organized in a two-level classification system based on specific criteria to assist in better classification and correlation of their respective incidents. This matching will enable better monitoring, handling and moderate cybercrime incident occurrences. The ultimate objective is to incorporate the schema-based description of cybercrime elements to a complete incident management system with standard operating procedures and protocols

***Keywords*— *System analysis and design, Supervised learning technique, Cyber security, Profiling, Web application*.**

I. INTRODUCTION

The advancements in computer systems and networks have created a new environment for criminal acts, widely known as cybercrime. Cybercrime incidents are occurrences of particular criminal offences that pose a serious threat to the global economy, safety, and wellbeing of society. Cybercrime involves a blend of diverse typical crimes with new illegal acts. Individual cybercrime incidents are occurrences of particular criminal offences and, as multiple national crime statistics and surveys demonstrate, are steadily increasing. According to the Federal Bureau of Investigation, the Internet Complaint center received 269422 complaints of Internet crime in 2014, which indicates a rise of 1600% in comparison to the 16838 complains.

Worldwide study released Pricewater house Coopers [3], the number of reported information security incidents around the world rose 48% in 2014, the equivalent of 117 339 attacks per day. Due to its complex nature, a series of definitions of cybercrime exist in literature and in different agencies responsible to tackle it. The U.S. Government does not have any certified definition of cybercrime that distinguish it from common criminal offences. Similarly, there is not a definition of cybercrime that differentiates it from other forms of cyber threats, and the term is often used interchangeably with other Internet- or technology-linked malicious acts such as cyber warfare, and cyber terrorism.

Gordon and Ford [7] proposed a typology consists of two categories. Type I offences characterize singular or discrete events facilitated by the introduction of malware programs such as keystroke loggers, viruses, and root kits. Type II offences are facilitated by programs that are not classified as crime ware, and they are generally repeated contacts or events from the perspective of the user. A much broader classification was recommended by Wall [8] proposing three distinct categories. The first is *Computer Integrity Crimes* including the illegal activities of cracking, hacking and denial of service (DoS). In the second category of *Computer-Assisted Crimes* the offences of virtual robberies, scams, and thefts are added. The third category is *Computer Content Crimes* including pornography, violence, and offensive communications. This paper aims to contribute towards better understanding cybercrime by proposing a schema-based cybercrime incident description that:

1) Identifies the features of a cybercrime incident and their potential elements and

2) Provides a two-level offence classification system based on specific criteria. The proposed schema can be extended with a list of recommended actions, corresponding measures.

II. PROPOSED APPROACH

The issues with providing a comprehensive description about cybercrime incidents are listed as follows:

1) There is already an adversity in existing cybercrime definitions that focus on different aspects.
2) The incidents that can be classified as cybercrime demonstrate a significant variety in their features an characteristics (e.g., offender, target, and means of attack).

To tackle the issues above has been proposed a hybrid schema-based incident description has been proposed which adapts accordingly to encompass and describe accurately the various cybercrime incidents. Having such a mechanism enables: 1) a better understanding of a particular incident; 2) accurate classification and monitoring of the corresponding criminal offence; and 3) effective action in terms of counter-measures and policy generation.

Which has been introduced an offence classification system based on two levels. The first level consists of the four different types of cybercrime offences introduced in the Convention on Cybercrime with the authors' addition of a new type: the combinational offences. For each level-1 offence type, there are level-2 subcategories based on further analysis by Gercke [1]. In these levels it consists of 5 types.

Table 1: Proposed Classification System of Cybercrime Offences

Level 1	Level 2
TYPE A Offences against the Confidentially, integrity and availability of computer data and systems	1. Illegal data access 2. Illegal data acquisition 3. Illegal interception 4. Misuse of data
TYPE B Computer related offences	1. Computer related forgery 2. Computer related fraud 3. Identity theft
TYPE C Content related offences	1. Child pornography 2. Religious Offences 3. Cyber bullying 4. Spam and related thefts
TYPE D Offences related to infringements of copyright and related rights	1. Copyright related offences
TYPE E Combinational offences	1. Cyber Warfare 2. Cyber laundering 3. Terrorist misuse of internet

.

This section presents a set of distinctive steps for the investigation of cybercrime incidents based on the proposed classification approach. The steps are as follows:

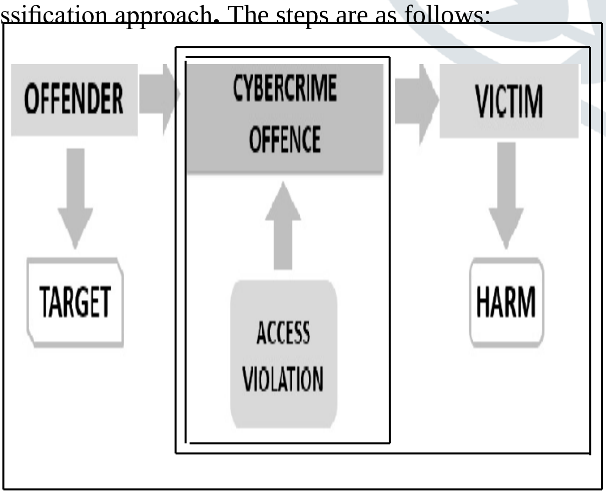

Fig 1: Basic Interrelations of the Cybercrime Features

Fig. 1 demonstrates the actual features and how they are interconnected.

1) The recipient of the cybercrime incident is the victim of the attack.
2) The motive of the subject represents the target of the offender and the outcome of the object is the harm inflicted on the victim of
3) the attack.
4) Lastly, the method of attack is the access violation of the cybercrime incident.

III. IMPLEMENTATION

The implementation of the Cybercrimes is explained in modules. They are

Incident Modules:

The first feature is a brief generic description of a particular incident that has occurred. Assigning it specific elements from a set of already occurring incidents would limit our capacity to describe new, future, or more sophisticated incidents. Therefore, this feature will remain generic and it will be further specified and clarified by the remaining of the proposed features.

Identified Offence Modules:

For an incident to be considered illegal, it has to be classified under an existing criminal offence. By grouping the various cybercrime incidents to corresponding offences the authorities can devise systematic and effective ways of tackling cybercrime in a timely manner. The challenge with cybercrime incidents is that they might include aspects of various known offences, they are complex in nature and they are still evolving in novel unprecedented occurrences.

Offender Modules:

The offender is the individual or entity that is responsible for carrying out or participating in a criminal incident. The offender can either be an individual, a group of individuals or an entity.

Access Violation Modules:

Access violation answers the question of how the incident took place. The authors' approach combines physical tampering with the logic of direct (overt)-indirect (covert) integrity threat of computer systems

Target Modules:

A cybercrime offender targets to specific values depending on the victim, the nature of the attack, and their objectives. These values are separated in two main categories, one regarding individual targets that refer to people or entities (e.g., companies and organizations), and the other one describing social targets like infra-structure and community.

Victim Modules:

A cybercrime victim is either individual when referring to a person, a company/organization, or a country/state that has been hurt, damaged, or suffered as a result of the offender's actions. The identified victims of computer-related offences are: 1) individual; 2) company/organization; and 3) country/state.

Harm Modules:

Harm lies at the core of traditional crimes such as murder, theft, assault and can also be inferred in computer-related offences due to similarities in nature. This harm is actual and discrete and can be inflicted to either human beings or entities. The nature of individual harm varies from moral harm, emotional distress and fear, when referring to people and to substantial damage and loss of property regarding entities.

IV. RESULT

The results of their classification are depicted by its graphical representations. The Fig 2 and 3 represents the Bar and Line representations of classification of Cybercrime Incidents which represents Web applications and the no of users who are responsible of Cybercrimes.

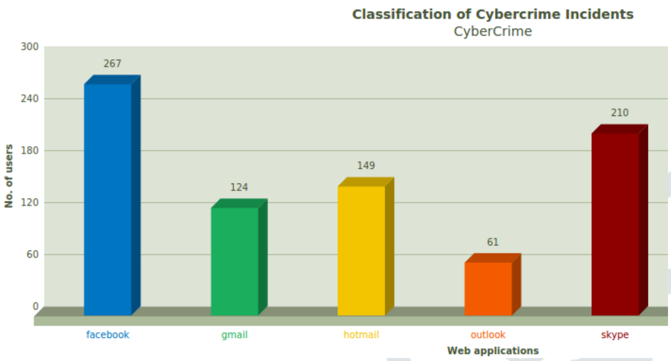

Fig 2: Bar representation of classification of Cybercrime Incidents

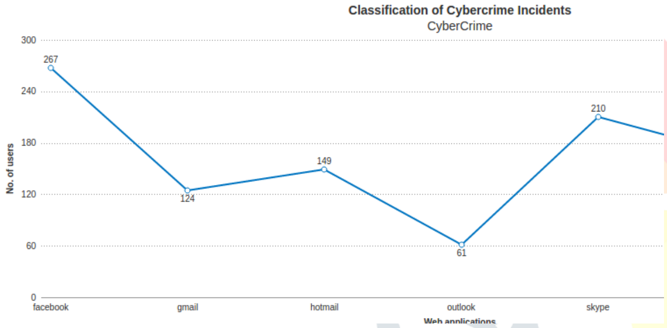

Fig 3: Line representation of classification of Cybercrime Incidents

The Fig 4 represents the 3D Pie representation of Cybercrime Incidents where we can clearly see the most affected Web applications such as the severity is more in Face book, the next is the Skype and the last is the twitter.

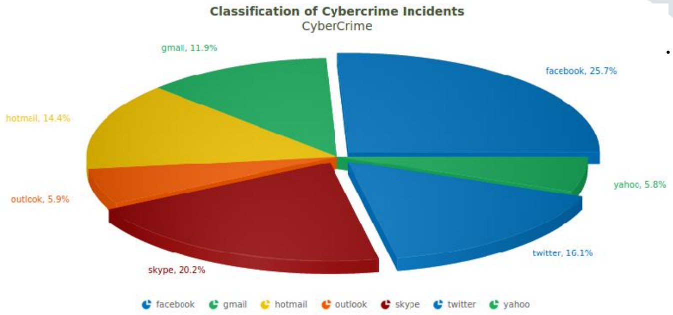

Fig 4: 3D Pie representation of Cybercrime Incidents

V. CONCLUSION

The identification of cyber crime features allows for a more comprehensive description of individual incidents that leads to better understanding, handling and management of their occurrences. The modular feature-based approach toward description of incidents allows for additional features to be included in the future. Also the expansion of their respective elements can also be achieved depending on specific perspectives. This paper also proposed a comprehensive two-level classification system of cybercrime offences. The system encompasses the most common forms of computer related offences and can be useful for law enforcement agencies.

The end result is an approach toward describing cybercrime incidents utilizing a systematic approach that can lead to: 1) better understanding of the specific incidents; and 2) better investigation of the specific elements involved in each respective case.. There is also ongoing research to introduce a new feature in the schema, regarding specific actions, counter measures and policies based on the offence type, and taking into consideration the incident occurrence frequency. The severity, urgency, and typical characteristics of the identified cybercrimes, require different preventive measures toward mitigation, while the same applies for the actions needed during crime conduction, and policies implemented in national or international level.

REFERENCES

[1] Adedayo M Balogon and Tranoszuva. IEEE Conference Publications (19-21 July 2017), **INSPEC Accession Number:** 17138028

[2] 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)

[3] 2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security

.

[4] IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 40, No. 4, July 2010

[5] D. L. Shinder and M. Cross, *Scene of the Cybercrime*. Burlington, MA, USA: Syngress, 2008

[6] FBI and NW3C. (May 22, 2015). *2014 Internet Crime Report*. Accessed on May 17, 2016. [Online]. Available: https://pdf.ic3.gov/ 2014_IC3Report.pdf

[7] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *J. Comput. Virol.*, vol. 2, no. 1, pp. 13–20, 2006.

[8] D. Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, U.K.: Polity, 2007.

APPENDIX

[1]	[2]	[3]
A cybercriminal profiling methodology with a hybridized deductive-inductive approach is used in this.	1. Cert-In:- Indian Computer Emergency Response Team 2. National Informatics Centre (NIC) 3. National Information Security Assurance Program (NISAP)	Supervised lEarning-Based Secure Information Classification and Decision Tree-based Risk Prediction (DTRP) algorithm are used
Advantages: This explores more efficient and investigative techniques of cybercriminal profiling. **Disadvantages:** The single cybercriminal profiling methodology is not expected to address all the issues highlighted above, it should be able to address the most significant ones	**Advantages**: It provides coordination and cooperation among all countries of the world for security of cyberspace. **Disadvantages:** Present laws are not efficient enough for preventing the cyber threats and there is a great urge for rectification of these laws and needs to be check timely and modify according to the betterment of Indian Society.	**Advantages:** This had proved that our scheme could perform good in Precision examinations. **Disadvantages**: This may not work with additional workload and only applicable in financial big data