A Systematic Approach Towards Classification and Description of Cyber Crime Incidents

[1]Dulam Bhavya Sree, [2]K. Satyanarayan Reddy
[1]MTech, [2]Professor & HOD
[1]Department of Computer Science, [2]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 paper 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

Keywords— System analysis and design, Supervised learning technique, Cyber security, Profiling, Decision Tree-based Risk Prediction.

I. INTRODUCTION

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 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 proposing three distinct categories. The first is *Computer Integrity Crimes* including the illegal activities of cracking, hacking and denial of service (DoS)[5]. 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. LITERATURE SURVEY

A. Open issues in Cybercriminal Profiling

A cybercriminal profiling methodology with a hybridized deductive-inductive approach consists of phases. The first phase adopts the behavioural evidence analysis framework to deductively generate a criminal profile. Certain characteristics in the profile – like the modus operandi and signature – are then used in an inductive approach for comparisons with the profile contents of known and solved cybercrimes. It was argued that this approach would be ardent at identifying offenders involved in multiple or organized cybercrimes, since their distinguishing characteristics would be flagged in the second phase of the methodology

Advantages:

This explores more efficient and investigative techniques of cybercriminal profiling.

Disadvantages:

The single cybercriminal profiling methodology is not probable to address all the issues highlighted above; it should be able to address the most significant ones only.

B. Recommendations for Effective Cyber Security Execution

Now-a-days, with the expansion of internet usage, cyber security is not restricted to a personal workstation, but also used to restrain information of personal mobile devices like tabs and cell phones because they have become very imperative medium of information transfer due to the current advancements in technology. In order to resolve cyber security issues, the security

researcher's community including government sector, academia, private sector must work together to understand the emerging threats to the computing world.

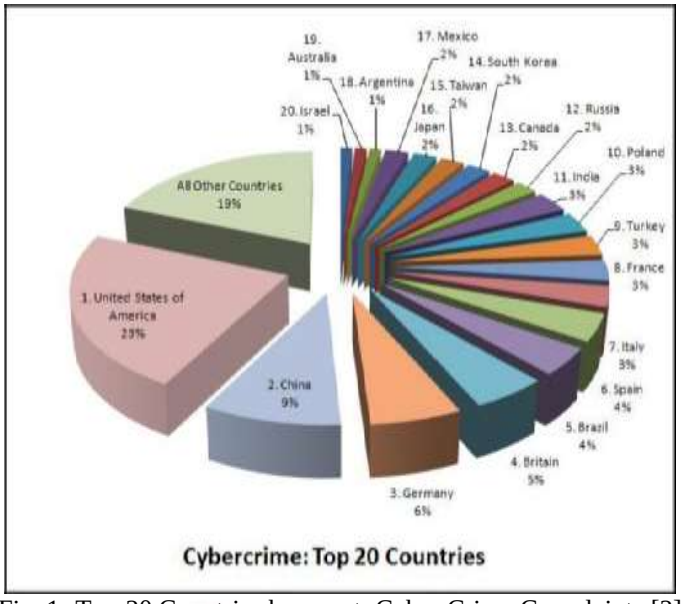

Fig. 1- Top 20 Countries by count: Cyber Crime Complaints [2]

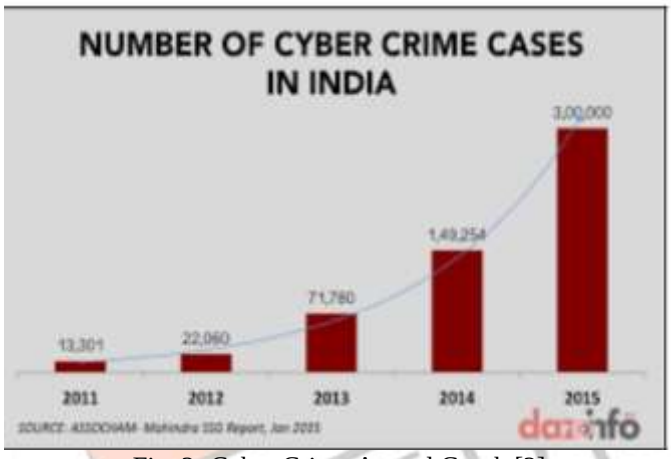

Fig. 2- Cyber Crime Annual Graph [2]

Figure 1 and 2 shows the top 20 countries cyber crime complaints and the cyber crime annual graph of India, as it is increasing day by day so there is a need to have a cyber security to us and our devices.

Objectives

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
2. To create an assurance framework for design of security policies and promotions and their enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
3. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing and validation of security of such product.
4. To provide fiscal profit to businesses for adoption of standard security practices and processes.
5. To enable Protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
6. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of low.

Advantages:

It provides co-ordination 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 refinement of these laws and needs to be checked timely and modify according to the development of Indian Society.

C. Security Aware Classification and Management in Financial Big data

Sharing data between financial service institutions has become an option of achieving value enhancements. However, the concern of the privacy information leakage has also arisen, which impacts on both financial organizations and customers. It is important for stakeholders in financial services to be aware of the proper information classifications, by which determining which information can be shared between the financial service institutions**.**

The proposed model is entitled as Supervised lEarning-Based Secure Information Classification (SEB-SIC) model, which is mainly supported by the proposed Decision Tree-based Risk Prediction (DTRP) algorithm. The proposed scheme is a predictive mechanism that uses the past data as the training dataset.

This creates a secure mechanism that distinguishes data for the purpose of protecting privacy information. This goal will be achieved by using supervised learning techniques to predict whether the information sharing will be hazardous for any relevant parties.

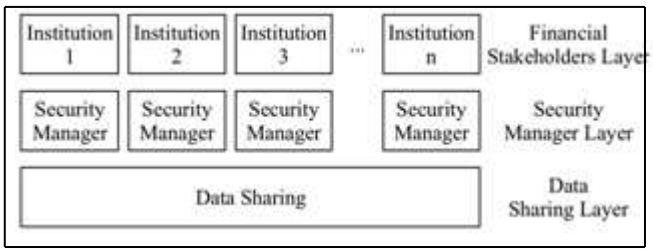

Fig 3: The three-layer architecture of the proposed SEB- SIC model [3].

Advantages:

This had proved that the scheme could perform well in Precision examinations.

Disadvantages:

This may not work with additional workload and only applicable in financial big data.

III. 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 and 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

IV. APPLICATIONS OF THE PROPOSED APPROACH

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:

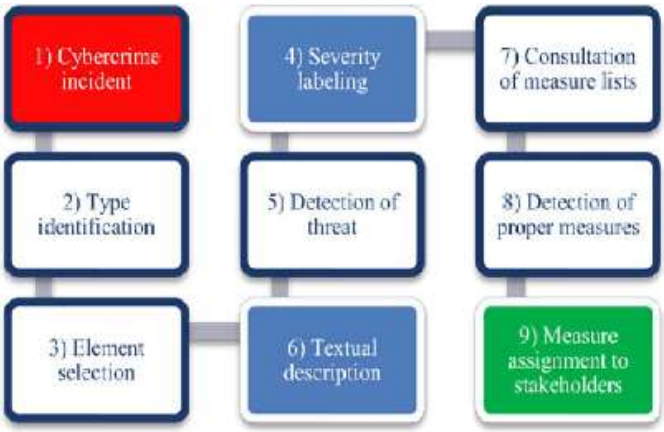

Fig 3: Stages toward the application of the proposed approach

1) The first step of implementation confirms the cybercrime incident and classifies it under an existing criminal offence.
2) The second step locates the type of the identified offence based on the proposed classification system
3) The schema-based visual description highlights which features are relevant to the particular offence. This step involves the selection of the unique elements that fit the particular incident.
4) In the next step, a detailed description of the offence incident is produced by merging the textual schema based incident description with the elements of the incident under examination.
5) The next step involves the detection of the exact threat that caused the offence.
6) The severity labelling of offences aims to formally assess the threat for prevention, evaluation and gathering of cybercrime statistics after crime commitment.
7) The next step involves extensive review of conducted lists of stakeholders, preventive measures and response actions for the offence type of the investigated incident
8) The fitting actions and measures could be detected and singled out, along with the involved stakeholders.
9) Lastly, the recommendations would be assigned to the proper stakeholders.

V. CONCLUSION

In this work has been proposed an introduction to comprehensive two-level classification system and 5 types of cybercrime offences. In this short paper, we provide an introduction of cyber crimes. We are planning to provide a more shallow analysis for the above-mentioned approach in the upcoming papers.

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

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	**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	**Advantages:** This had proved that our scheme could perform good in Precision examinations. **Disadvantages**: This may not work with additional workload and only

most significant ones	timely and modify according to the betterment of Indian Society.	applicable in financial big data