A Systematic Approach towards Classification and Description of Cyber Crime Incidents

Y Madhu[1], Mylapoor Madhu[2]
[1]*Student, Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, India*
[2]Asst.Professor, *Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, India*

***Abstract*- 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 well-being of society. This paper offers a comprehensive understanding of cybercrime incidents and their corresponding offences combining a series of approaches reported in relevant literature. Initially, this paper reviews and identifies the features of cybercrime incidents, their respective elements and proposes a combinatorial incident description schema. The schema provides the opportunity to systematically combine various elements--or cybercrime characteristics. Additionally, a comprehensive list of cybercrime-related offences is put forward. The offences are ordered in a two-level classification system based on specific criteria to assist in better classification and correlation of their respective incidents. This enables a thorough understanding of the repeating and underlying criminal activities. The proposed system can serve as a common reference overtaking obstacles deriving from misconceptions for cybercrimes with cross-border activities. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that match with the offence type and subsequently with a particular incident. 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.**

***Index Terms*- System analysis and design, Supervised learning technique, Cyber security, Profiling, Decision Tree-based Risk Prediction.**

I. INTRODUCTION

The evolution of computer systems and networks besides enhancing our lives has created a new environment for criminal acts, widely known as cybercrime. Cybercrime combined with the use of internet to form a mixture of diverse typical crimes with some new illegal acts. Individual cybercrime incidents Cyber security Ventures expects 2018 to be the "Year of Security Awareness Training" — the breakthrough year when organizations globally take the (financial) plunge and either train their employees on security for the first time or double down on more robust and ongoing security awareness programs. Global spending on security awareness training for employees is predicted to reach $10 billion by 2027, up from around $1 billion in 2014. Training employees how to recognize and defend against cyber attacks is the most under spent sector of the cyber security industry.

II. LITERATURE SURVEY

Open issues in Cybercriminal Profiling A cybercriminal profiling methodology with a hybridized deductive-inductive approach consists of phases. The first phase adopts the behavioral 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 Cyber security Ventures predicts that there will be 6 billion Internet users by 2022 (75% of the projected world population of 8 billion) — and more than 7.5 billion Internet users by 2030 (90% of the projected world population of 8.5 billion, 6 years of age and older). Like street crime, which historically grew in relation to population growth, we are witnessing a similar evolution of cybercrime. It's not just about more sophisticated we aponry, it's as much about the growing number of human and digital targets. Microsoft helps frame digital growth with its estimate that data volumes online will be 50 times greater in 2020 than they were in 2016. 'The Big Data Bang' is an IoT world that will explode from 2 billion objects (smart devices which communicate wirelessly) in 2006 to a projected 200 billion by 2020, according to Intel. Gartner forecasts that more than half a billion wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearable's include smart watches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

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 Earning-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.

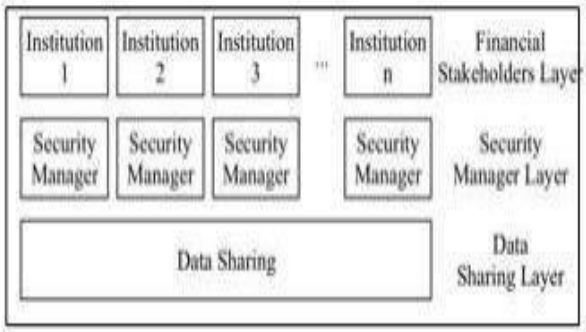

Fig 3: The three-layer architecture of the proposed SEB- SIC model [3]. Advantages: This had proved that the scheme could perform well in Precision examinations. Disadvantages: This may not work with additional workload and only applicable in financial big data.

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

(4) each level-1 offence type, there are level-2 subcategories based on further analysis by Gerick[1]. In these levels it consists of 5 types.

Level 1	Level 2
TYPE A Offences against the Confidentiality, 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

(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 labeling 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.

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.

V. CONCLUDE

In this work has been proposed an introduction to comprehensive two-level classification system and five types of cybercrime offences..

REFERENCES

[1] 2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016)
[2] 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
[3] 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