IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA-DRIVEN DECISION SUPPORT FOR OPTIMIZING CYBER FORENSIC INVESTIGATIONS

S.Jonisha[1] , E Sharran[2], S Vignesh[3] ,AR .Sibi[4]

Assistant Professor[1] , Student[2,3,4]

Department of Computer Science and Engineering

PERI INSTITUTE OF TECHNOLOGY

Abstract

The venture known as "Data-Driven Decision Support for Optimizing Cyber Forensic Investigations" is a web based application. This software provides facility for confirming criminal offenses, Problems, losing individuals to DIG. This software provide facility for reporting online crimes, online complaints, missing persons show criminal list and details on web page. Any number of public can complaint through online. Each user first makes their login to server to share their availability. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the unit, whether those functions include high-technology crime investigations, evidence collection, or forensic analysis. However, Cyber forensic contains steps to investigate or collect the data It is defined as the processes and tools used in investigations and gathering evidence. Some of the instruction will be provided as a default such as category wise. By analysing the investigation report, process will be optimized to reduce the investigation process.

Introduction

Modern science and technology has revolutionised the field of crime solving and has made the process much faster and more reliable. The word Forensic refers to all the science and technology used in the solving of crime. The aim of this Forensic Management System is to manage the large volumes of data that are produced in the process of solving crimes by the application of scientific methods and modern technology. When creating a new case file the system will be able to store specific information in categories. This system can be used to easily collaborate on case files, temporary user profiles can be created if the other department does not implement this system.

Literature survey

Cyber Threat Intelligence – Issue and Challenges

Today threat landscape evolving at the rapid rate with much organization continuously face complex and malicious cyber threats[1]. Cybercriminal equipped by better skill, organized and well-funded than before. Cyber Threat Intelligence (CTI) has become a hot topic and being under consideration for many organization to counter the rise of cyber-attacks. The aim of this paper is to review the existing research related to CTI. Through the literature review process, the most basic question of what CTI is examines by comparing existing definitions to find common ground or disagreements. It is found that both organization and vendors lack a complete understanding of what information is considered to be CTI, hence more research is needed in order to define CTI. This paper also identified current CTI product and services that include threat intelligence data feeds, threat intelligence standards and tools that being used in CTI. There is an effort by specific industry to shared only relevance threat intelligence data feeds such as Financial Services Information Sharing and Analysis Center (FS-ISAC) that collaborate on critical security threats facing by global financial services sector only.

While research and development center such as MITRE working in developing a standards format (e.g.; STIX, TAXII, CybOX) for threat intelligence sharing to solve interoperability issue between threat sharing peers. Based on the review for CTI definition, standards and tools, this paper identifies four research challenges in cyber threat intelligence and analyses contemporary work carried out in each. With an organization flooded with voluminous of threat data, the requirement for qualified threat data analyst to fully utilize CTI and turn the data into actionable intelligence become more important than ever. The data quality is not a new issue but with the growing adoption of CTI, further research in this area is needed.

Unknown Attack Detection Based on Zero-Shot Learning

In recent years, due to the frequent occurrence of network intrusions, more and more researchers have begun to focus on network intrusion detection. However, it is still a challenge to detect unknown attacks[2]. Currently, there are two main methods of unknown attack detection: clustering and honeypot. But they still have unsolved problems such as difficulty in collecting unknown attack samples and failure to detect on time. Zero-Shot learning is proposed to deal with the problem in this article, which can recognize unknown attacks by learning the mapping relations between feature space and semantic space (such as attribute space). When the semantic descriptions of all attacks (including known and unknown attacks) are provided, the classifier built by Zero-Shot learning can extract common semantic information among all attacks and construct connections between known and unknown attacks. The classifier then utilizes the connections to classify unknown attacks although there are no samples for unknown attacks. In this article, we first propose to use Zero-Shot learning to overcome the challenge of unknown attack detection and illustrate the feasibility of this method. Secondly, we then propose a novel method of Zero-Shot learning based on sparse auto encoder for unknown attack detection.

Real-time Attack Scenario Reconstruction from COTS Audit Data

We present an approach and system for real-time reconstruction of attack scenarios on an enterprise host. To meet the scalability and real-time needs of the problem, we develop a platform-neutral, main-memory based, dependency graph abstraction of audit-log data. We then present efficient. This paper describes a focused literature survey of machine learning (ML) and data mining (DM) methods for cyber analytics in support of intrusion detection. Short tutorial descriptions of each ML/DM method are provided. Based on the number of citations or the relevance of an emerging method, papers representing each method were identified, read, and summarized. Because data are so important in ML/DM approaches, some well-known cyber data sets used in ML/DM are described. The complexity of ML/DM algorithms is addressed, discussion of challenges for using ML/DM for cyber security is presented, and some recommendations on when to use a given method are provided.

Around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. Data mining methods are proposed for cyber analytics in support of intrusion detection.[1]., tag-based techniques for attack detection and reconstruction, including source identification and impact analysis. We also develop methods to reveal the big picture of attacks by construction of compact, visual graphs of attack steps. Our system participated in ared team evaluation organized by DARPA and was able to successfully detect and reconstruct the details of their team's attacks on hosts running Windows, Free BSD and Linux[2].

This method maps the feature of known attacks to the semantic space, and restores the semantic space to the feature space by constrains of reconstruction error, and establishes the feature to semantic mapping, which is used to detect unknown attacks. Verification tests have been carried out by using the public dataset NSL_KDD. From the experiments conducted in this work, the results show that the average accuracy reaches 88.3%, which performs better than other methods.[3].It also can serve an audit trails for extending as possible in the process of investigating the target machines. In addition, processes running can give a good review to show a full list of all processes running on the suspicious machine [9]. This reviewing will help examiners in detecting malicious process and abnormal activities. The evidence collected from the forensic investigation is the data stored in the digital systems and it could be deleted files, hidden files, metadata, corrupted data, hard drive data, in-memory data, or any other forms of data [4].

Digital forensics (computer forensics) is a discipline used to search digital evidence with scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources to enable successful prosecution. The goal of digital forensics is to obtain legal evidence found in digital media [4] The initial process of digital forensic namely the phase of data acquisition, which is the phase in which investigators make a perfect copy of the storage medium and Random Access Memory [5]. Investigators should be aware of all the changes data quickly. One barrier may be that cases are dismissed due to insufficient evidence, which reinforces the invulnerability of perpetrators.

SYSTEM DESIGN

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

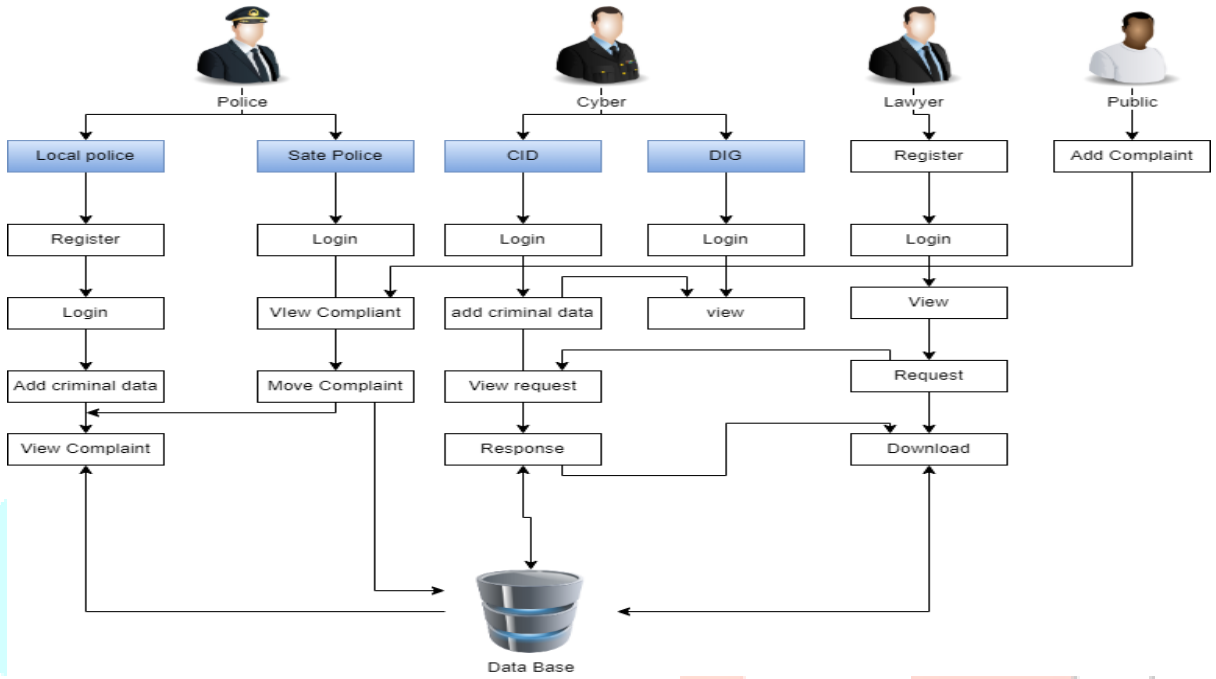

Fig 1: system design

IMPLEMENTATION

This chapter describes the implementation of searched based application. It deals with the source code for main viewpoint for Anonymous Database Management.

MODULES

- **REGISTER**
- **LOGIN**
- **CID**
  - ADD CRIMINAL DATA
  - VIEW LAWER REQUEST
- **DIG**
  - MAINTAIN CRIMINAL DATA
  - RESPONSE TO LAWER
- **STATE POLICE**
  - APPROVE REGISTERATION
  - VIEW PUBLIC COMPLAINT
  - MOVE LOCAL STATION

- **LOCAL POLICE**
  - ADD CRIMINAL DATA
  - VIEW STATE POLICE FILES
  - MAKE REPORT
- **PUBLIC ADD COMPLIANT**
- **LAWYER**
  - VIEW THE LOCAL POLICE DATA
  - REQUEST CRIMINAL DATA
  - DOWNLOAD CRIMINAL DATA

MODULE DIAGRAM

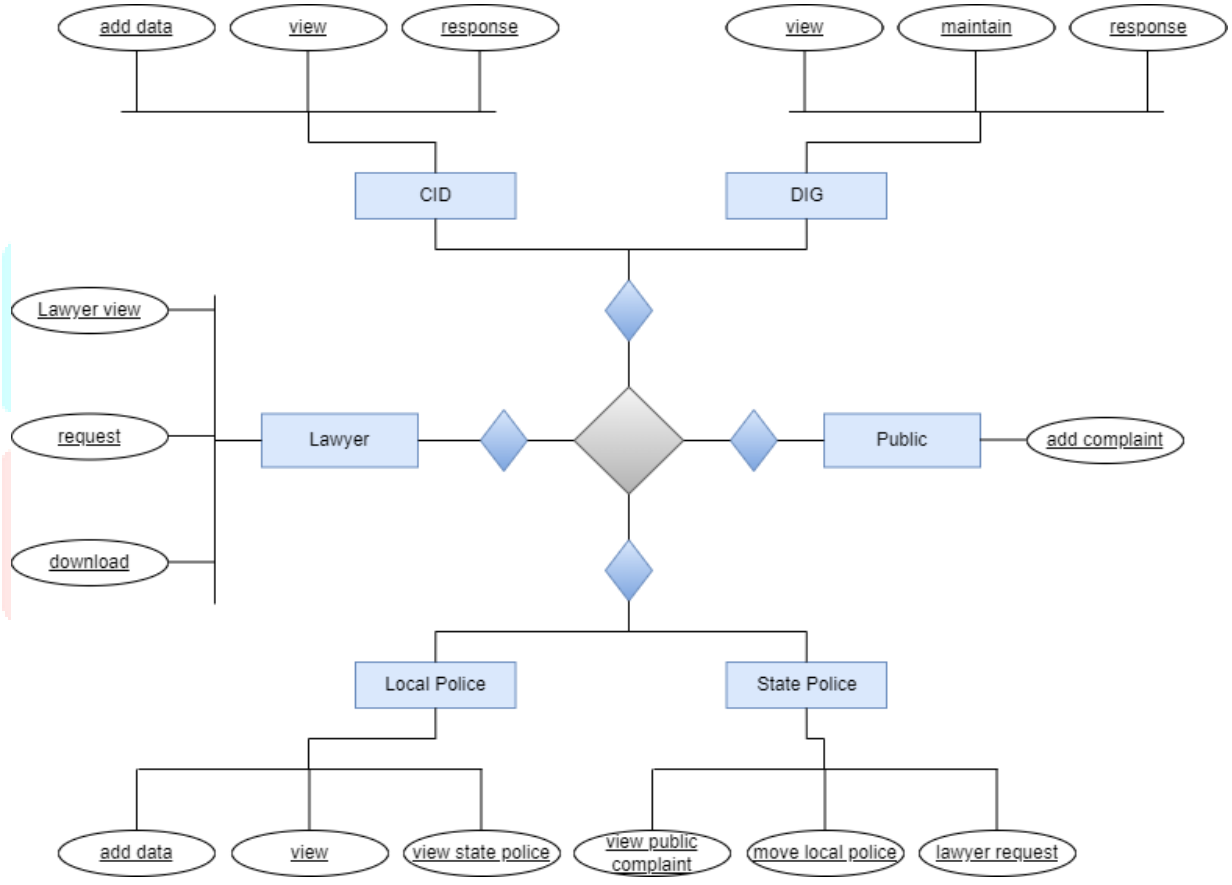

Fig 2:Data flow process

CONCLUSION

Digital forensics involves the process of identifying, collecting, acquiring, and preserving. Analysing, and presenting of digital evidence. Digital evidence must be authenticated to ensure its admissibility in a court of law. Ultimately, the forensic artefacts and forensic methods used to static or live acquisition depend on the cases and its section. Real evidence must be competent (authenticated), relevant, and material. This software is developed with modular approach. All module in this system have been tested with valid data and everything worked successfully.

REFERENCE

[1] K. Finnerty, S. Fullick, H. Motha, J. N. Shah, M. Button, and V. Wang,"Cyber security breaches survey 2019," Dept. Digit., Culture, MediaSport, London, U.K., Tech. Rep., Apr. 2019.

[2] *Cost of a Data Breach Report 2019*, IBMSecurity, New York, NY, USA,2019.

[3] A. Brinson, A. Robinson, and M. Rogers, "A cyber forensics ontology:Creating a new approach to studying cyber forensics," *Digit. Invest.*,vol. 3, pp. 37–43, Sep. 2006.

[4] L. Martin. (2014). *Cyber Kill Chain*. [Online]. Available: http://cyber.lockheedmartin.com/hubfs/GainingAdvantageCyberKillChain.pdf

[5] V. Diaz, D. Emm, and C. Raiu, "Kaspersky security bulletin 2019:Advanced threat predictions for 2020," Kaspersky Lab., Moscow, Russia,Tech. Rep., 2019.

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integratingforensic techniques into incident response," *NIST Special Publication*,vol. 10, no. 14, pp. 800–886, 2006.

[7] J. Williams, "Acpo good practice guide for digital evidence," Metrop.Police Service, Assoc. Chief Police Officers, GB, London, U.K.,Tech. Rep., Mar. 2012.

[8] V. S. Harichandran, F. Breitinger, I. Baggili, and A. Marrington,"A cyber forensics needs analysis survey: Revisiting the domain's needsa decade later," *Comput. Secur.*, vol. 57, pp. 1–13, Mar. 2016
.
[9] S. Barnum, "Standardizing cyber threat intelligence information with thestructured threat information expression (STIX)," *Mitre Corp.*, vol. 11,pp. 1–22, Jan. 2012.

[10] J. Navarro, A. Deruyver, and P. Parrend, "A systematic survey on multistepattack detection," *Comput. Secur.*, vol. 76, pp. 214–249, Jul. 2018.