Mobile Application Category Cybercrime To Filter The Content Using Ontology

M A Kintani[1], U Rizal[1]
[1] Information System, Computer Science Faculty, Bandar Lampung University, Indonesia

1. Introduction

1.1Background

The current Internet is growing rapidly. This has created new opportunities in various fields which we can think of, be it entertainment, business, sports or education. The Internet is a useful way for people to do business effectively, very fast. It saves a lot of time, money and resources. Unfortunately, it is also an open invitation to fraudsters and online scams becoming more rampant. Like two sides of a coin, the Internet also has its own drawbacks. One of the major disadvantages is Cybercrime - illegal activities on the Internet. Computers today are being misused for illegal activities such as e-mail fraud, credit card fraud, spam, piracy of software and so forth, which violates privacy.

Cybercrime is a crime where a criminal act can only be done with the use of cyber technology and occur in the cyberworld. (M.Yoga.P,2013).The ontology is defined as a formal and clear picture of conceptualization together. (Gruber 1993). Frantz and Franco (2005) argued that ontology provide shared and common understanding of the domain to be notified between people and computers to facilitate knowledge sharing and reuse. In addition, Frantz and Franco explained that ontology provides a clear formal conceptualization (ie the meta-information) that describes the semantic information of the arrest of a static domain knowledge-based systems.Ontology is proposed to collect, examine, analyze, prepare for, obtain and store evidence of computer crime in cyberspace. To answer the above conditions and problems, then here I do resume journal entitled **"Analysis and Classification of Cybercrime with *Ontology*Method".**

2. Theoretical

2.1 Literature

A. Review of the literature obtained from the first journal entitled **Towards a Comprehensive Ontology Based Investigation** is written by Amir Mohamed Talib, Fahad Omar Alomary of Information Technology Department, College of Computer and Information Sciences at Al-Imam Muhammad Ibn Saud Islamic University, Riyadh, Kingdom of Saudi Arabia (KSA), (2015). In the study Ontology method is proposed to determine the difficulty associated types of digital crime and evidence collection in the case of digital forensics. Ontology development consists of three main steps, 1) domain, objectives and setting the scope, 2) the acquisition of important terms, the class and the class hierarchy conceptualization and 3) the creation of examples.In this study, the Web Ontology Language (OWL) [14], [15] which was chosen to represent the ontology security because of its power to reveal the meaning and semantic and complex relationships. OWL is a fundamental concept in class, individuals and property.Protegehelp the development of ontology, using text mining and natural language processing to extract the relevant terms of the scientific literature that can then be arranged, protege enables designers vocabulary to capture, repair and eventually formalize the intuition without being forced to deal with the disturbing logical details early in the design process.

B. Review of the literature obtained from the second journal, entitled **A Study on Significance of Event Web Ontology Approach in Crime Mining** which was written by Megha Mudholkar, Ujwala Bharambe of *Thadomal Shahani Engineering College, Mumbai, Maharashtra,*India,(2013). In that study a lot of crime information in the document explained by events, event-based semantic technology can be used to study crime patterns and trends of web-oriented. So for mining cyber crime, ontology built to extract attributes and relationships in the web page and reconstruct scenarios for mining crime.This study explores cyber crime in various construction event web page

with ontology. For example, the mechanism is designed, implemented and evaluated that allows us to define and information mining interest. In particular, the event ontology is defined and show how it can be used to describe cyber crime at the level of events, relationships and class events. Procedure-based cyber crime mining event that the proposed ontology concerns prehandling web text, feature extraction, feature reconstruction and crime mining. This paper discusses the scope of the build event ontology for web crime focused on the mining and quarrying attributes and relationships in the web page.

C. Review of the literature obtained from journals third, entitled **An ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence** that was written by Jasmin Cosic from the *Ministry of the Interior of Una-sana canton, IT Section of the Police Administration, Bihac, B &*H.By Zoran Cosic of *"STATHEROS", doo Kastel Stari, Split,Croatia.* By Miroslav Baca of *the University of Zagreb, Faculty of Organization and Informatics Varazdin, Croatia,* (2011). In the study, the purpose of the paper is to develop ontologies to provide a new approach to study and better understand the marketing chain of digital evidence. In addition, the developed ontology can be used as a method to further develop a set of standards and procedures for the safe management of digital evidence.

3. Results and Discussion

From the results of previous studies, obtained ratio as follows:

Table 1. Comparison 3rd Journal

Peneliti dan Tahun	Judul Jurnal Penelitian	Metode	Hasil
Amir Mohamed Talib dan Fahad Omar Alomary (2015)	Towards a Comprehensive Ontology Based-Investigation for Digital Forensics Cybercrime.	Ontology Web Language (OWL) digunakan untuk keamanan ontology karena kekuatannya untuk mengungkapkan makna dan semantic hubungan yang kompleks. Konsep dasar dalam OWL adalah kelas, individu, dan properti. Dan menggunakan Protégé untuk membantu pengembangan ontology, menggunakan teks mining dan pengolahan bahasa alami untuk mengekstrak istilah yang relevan dari literatur ilmiah.	Pada jurnal ini, ontology forensik digital yang dihasilkan dari proses protégé, memiliki 180 kelas utama dan 179 sub kelas. Sebuah ontology berbasis OWL dengan konsep inti forenisik digital aset, forensik digital analisis, proses forensik digital model dan kebijakan digital forensik. Semua konsep inti adalah subclass untuk menyediakan kosakata domain digital forensik.
Megha Mudholkar dan Ujwala Bharambe (2013)	A Study on Significance of Event Ontology Approach in Web Crime Mining	Ontology dibangun untuk mengekstrak atribut dan hubungan di halaman web dan merekonstruksi skenario untuk web mining.	Penelitian ini mengeksplorasi kejahatan cyber di berbagai laman web dengan konstruksi ontology. Dan terfokus pada penggalian atribut dan hubungan dihalaman web.
Jasmin Cosic, Zoran Cosic dan Miroslav Baca (2011)	An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence.	Ontology adalah metode yang akan membantu untuk lebih memahami dan mendefinisikan bukti forensik digital. Tujuan utama nya adalah untuk mendefinisikan diagram taksonomi rantai pemasaran dari bukti digital yang akan menjadi titik pusat untuk kerja lebih lanjut pada penelitian ini.	Pada penelitian ini, dengan ontologi kita bisa berbagi pemahaman umum dari struktur domain forensik digital antara peneliti forensik dan pribadi lainnya yang ada hubungannya dengan bukti digital, antara agen perangkat lunak, antara penyidik forensik dan perangkat lunak. Hal ini juga dapat memungkinkan penggunaan kembali pengetahuan dalam proses penyidikan digital. The DCoDeOn (Digital Chain of Custody Digital Bukti Ontologi) dirancang dengan cara menyisipkan sederhana kelas baru (bagian). Slot (sifat) dapat didefinisikan dalam definisi kelas, kendala properti, aspek umum (kardinalitas, jenis nilai dll).

As an explanation, take a sample from one journal, entitled A Study on Significance of event in a Web Ontology Crime Mining Approach:

3.1 Building Web Ontology Oriented Event Crime

a. Category Cyber crime

According to the decision passed by the 'decision of the Standing Committee of the National People's Congress on maintaining the security of the Internet' on December 28, 2000, the crime using the internet as a tool can be divided into the following categories: (1) fraud; (2) Internet pornography; (3) Rade illegal; (4) false advertising; (5) breach of privacy; (6) abetting, inciting all kinds of evil; (7) gambling network; (8) damage to the reputation, credibility; (9) intimidation, extortion; (10) the claims; (11) are offensive, defamatory; and (12) other people, such as counterfeiting, illegal organizations, etc. However, cybercrime over always reflected on the web with different styles.

b. Develop Event Ontology Oriented Cyber Crime

1. Events in Relation

Base for the manufacture of the event ontology is the events and relationships. what elements are included events? different applications have different definitions. For cybercrime, analysts are most concerned about the type of event (denoted by action), participants, time, location, instruments, products involved, etc. Therefore, we use the structure of the six-tuple event.

Definition 1. An event refers to the things that happen at certain times and locations, which involve a number of actors and stuff, and use multiple tools. An event can be defined as a six-tuple: e = (A, C, T, L, F, G).The elements of an event called the six-tuple event elements, which is the act (A), participants (P), time (T), location (L), the tool (M) and goods (G) respectively. And participants involved subjects and objects.

Definition 2. relations events are divided into two categories: the relationship secret and non-secret relationship. Furthermore, non-confidential relationship is divided into the following categories: component relationships, causal relationship, follow the relationship, and the approval of the relationship [14].

Definition 3. An event class (EC) refers to a series of events that have the same characteristics.

3.2 Examples of events Ontology

In project, oriented events cybercrime ontology contain built 185 class event. Figure 1 is a fragment of the event ontology which contains five of the event classes and their relationships.

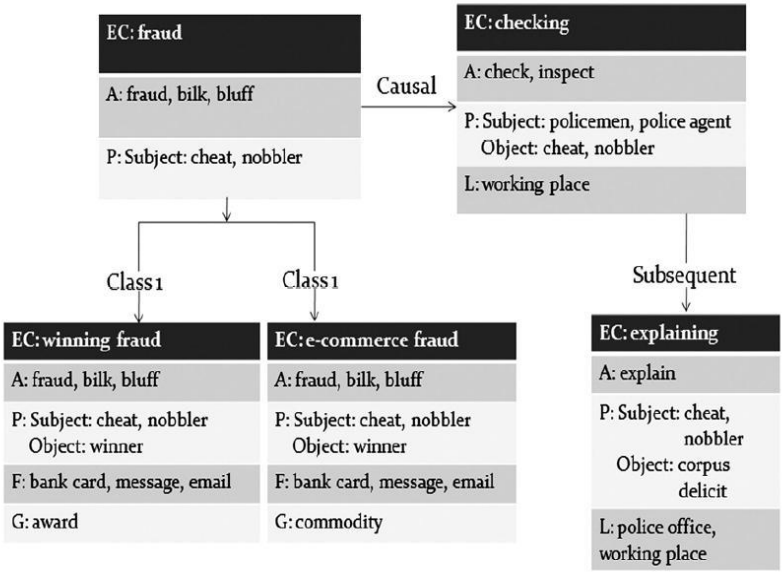

Figure 1. AFragment Event Ontology To Cyber Crimes

In Figure 1, the event class five domains are displayed: 'fraud', 'won a fraud', 'fraudulent e-commerce', 'check' and 'explain'. Typically, 'fraud' results 'check' and 'explaining' following 'check'. Because the 'winning fraud' and 'fraudulent e-commerce' is a sub-class of 'fraud', they will inherit the attributes of 'fraud'.Protege is used as a tool to build a cyber crime event ontology. OWL is used as a protégé ontology language. Figure 3.2 is a fragment of cyber crime event ontology hierarchy is built using Option OWLViz in PROTEGE 4.

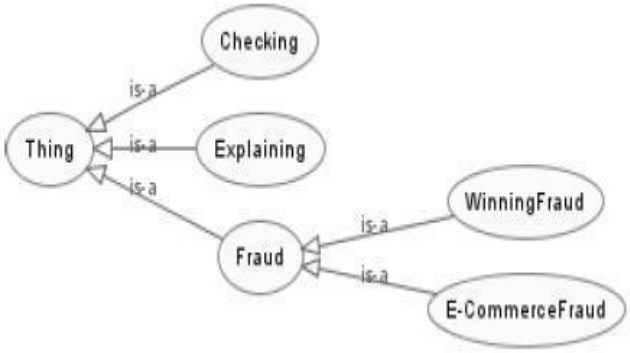

Figure 2. OWLViz featuring Hierarchy for cybercrime

To cybercrime mining application, event ontology built to extract attributes and relationships in the web page and also reconstruct the crime scenario for mining. Event ontology and Support Vector Machine (SVM) and Naïve Bayes classification is used to identify the different types of cyber crime. Figure 3. presents the entire process of mining crime ontology web based event.

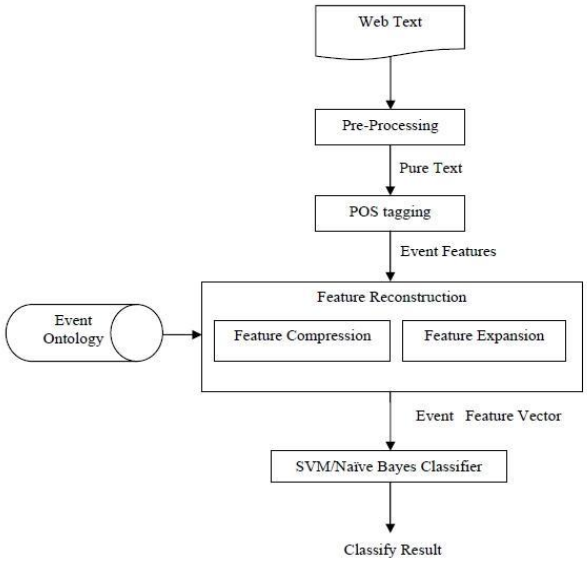

Figure 3. Process Overall Crime Mining Ontology Web Based Event

Processes in Figure 3. includes the following phases:

Phase 1: Pre-processing site Text (extracting web page content)

Most web text html format. After pre-processing, filtering URLs, ads and other information, pure text reserved.

Stage 2: Decision Feature Candidates (extract from the feature event texts)

After POS text tagging and filtering of stop-words, words that remains is pure text candidate features.

Stage 3: Reconstruction Feature (representing text with the feature event)

Reconstruction of features consists of compression and expansion features. Compression feature refers incorporates some features of ontology or thesaurus. And expansion refers to adding a number of features using ontology.

Stage 4: Data Mining

It contains many techniques such as clustering, classification, retrieval, discovery associative, and so on. Based on the above discussion, the authors will want to design an *application report* by capturing and reporting on internet sites that allegedly contain the contents *of*cybercrime.Here, after analysis of

the site report by Internet users, for the next decision will be submitted to the authorities (DISKOMINFO and police) whether the site is to commit cybercrime.

4. Conclusions and Recommendations

4.1 Conclusion

Based on the analysis discussion of previous research journals, it can be concluded:

A. Ontology can provide structure, the depiction of relationships, interactions, and the factors that influence by capturing content that is included in cybercrime.
B. Is expected by the *Reportapplication* that was built later can minimize the occurrence of *cybercrime* in particular to the city of Bandar Lampung.

4.2 Suggestions

Based on the results of research and discussion in the previous chapter there are some suggestions that can be given to the author for subsequent research:

A. Hopefully with the analysis of this study can be utilized by the user associated with the well.
B. Analysis of the previous chapter, the author may be implemented for future research.
C. The author realizes that this paper is not perfect, there are still a lot of shortcomings. for it is expected for other users to be able to develop it.

References

[1] Amir Mohamed Talib, FO 2013.*"Towardsa Comprehensive Ontology-Based Digital Forensics Investigation for Cybercrime"*. International Journal on Communications Antenna and Propagation (I.Re.CAP), **Vol. 5**, N.

[2] Jasmin Cosic, ZC, 2011.*"Anontological Approach to Study and Manage Digital Chain of Custody of Digital*Evidence".UDC 004 822: 004 056 Communications Preliminary Article, Submitted 03/11; Accepted 06/11, JIOS, **VOL. 35**, NO. 1 (2011).

[3] Megha Mudholkar, UB 2013.*"AStudy on Significance of Event Web Ontology Approach in Crime Mining"*. International Journal of Latest Trends in Engineering and Technology (IJLTET) **Vol. 2** Issue 2, ISSN: 2278-621X.

[4] Namosha Veerasamy, MG 2012.*"Buildingan Ontology for*Cyberterrorism".Taken from https://www.researchgate.net/publication/266055691_Building_an_Ontology_for_Cyberterrorism

[5] (2013), G. 2013. *Understanding Cybercrime According to the experts*. Taken from http://ogapermana.blogspot.co.id/2013/04/pengertian-cyber-crime-menurut-para-ahli_11.html Amardi, R .. 2013. Definitions Hackers and Crackers According to Experts. Taken from https://roniamardi.wordpress.com/definisi-hacker-cracker/

[6] Bumulo, DR 2017. *Carding Type Case Study Analysis By Experts.* Taken from http://akhirnyadennieskuliah.blogspot.co.id/2014/11/analisa-study-kasus-jenis-carding.html

[7] KBBI. 2017. *The meaning of the word Internet* - Indonesian Dictionary (KBBI) Online. Taken from http://kbbi.web.id/internet

[8] KBBI. 2017. *The meaning of Classification* - Big Indonesian Dictionary (KBBI) Online. Taken from http://kbbi.web.id/klasifikasi

[9] Kurniawan, A. 2013. *Analysis 13 Definition World 'According to the experts.* Taken from http://www.gurupendidikan.com/13-pengertian-analisis-menurut-para-ahli-didunia/

[10] Oktaviandy, N. 2012. *Research Methods Experiment.* Taken from https://navelmangelep.wordpress.com/2012/02/27/metode-penelitan-eksperimen/

[11] SURABAYA, IT 2007. *Understanding and Application of Experimental Methods in Research*. Taken from https://idtesis.com/metode-eksperimental/

[12] Syrozone, A. d. 2012. *Hackers and Crackers: Hacker*. Taken from http://kelompok1hackercracker.blogspot.co.id/2012/11/pengertian-hacker_2.html

[13] Trianto, M. 2013. *Methods According Sugiyono*. Taken from

http://rayendar.blogspot.co.id/2015/06/metode-penelitian-menurut-sugiyono-2013.html