**CyberCrime Attacks Ontology**

**Editors:** Anam Razaq, Syeda Moaddat Naqvi

**Abstract**

Cybercrime refers to an unlawful activity that specifically focus on computers, computer networks, or networked devices as tools or targets for criminal actions. Ontology is a way of describing the semantics of data about the subject. CyberCrime Attacks ontology represents the comprehensive knowledge about different attacks like their best defences, prevention and detection techniques and vulnerabilities. The purpose of ontology is to offer accessible information to individuals who are new to the field, students, and domain experts.

**Keywords:** Cybercrime, Ontology, Attacks, Defences, Prevention, Detection, Vulnerabilities.

1. **Introduction**

The emergence of cybercrimes can be traced back to the activities of hackers attempting to infiltrate computer networks. Some individuals pursued the thrill of infiltrating high-level security networks, while others aimed to acquire sensitive and classified information. In recent years, there has been an increase in cybercrimes, leading to negative consequences for individuals, organizations, and governments. A comprehensive understanding of cybercrime attacks is an imperative requirement for formulating suitable legal and policy measures to cybercrimes. Therefore, we developed CyberCrime attacks ontology that offers valuable insights for understanding and analyzing different types of cybercrime attacks. Attacks includes email attacks, encryption attacks, insider threat attacks, network attacks, physical attacks, social engineering attacks and software attacks. We have incorporated detailed information regarding each attack, including defence mechanisms, prevention techniques, detection techniques and vulnerabilities. For each attack, we have defined defence strategies that can be employed to safeguard against potential threats. These defences encompass a range of proactive measures, including the implementation of secure network configurations, encryption protocols.

Additionally, we have identified prevention techniques that focus on proactive actions to eliminate or minimize the likelihood of an attack occurring. These prevention measures can include regular security assessments, employee training program. Furthermore, we emphasized detection techniques designed to identify and alert against potential threats. These techniques includes intrusion detection systems, anomaly detection algorithms, and behavior analytics to monitor network traffic, system logs, unauthorized access attempts. We also addressed vulnerabilities associated with each attack. By highlighting these vulnerabilities, organizations can gain insights into potential weak points within their systems, software, or processes and take appropriate steps to address them promptly. We have included all aspect mentioned above in our ontology. We have used Protégé for ontology development. Other tools that we have used are as follows:

* ***Owl:***For ontology implementation.
* ***Web-vowel:*** For interactive visualization of ontology.
* ***Github:*** For publishing the ontology.
* ***WIDOCO:***For generating ontology documentation.
* ***SPARQL:***To query the ontology

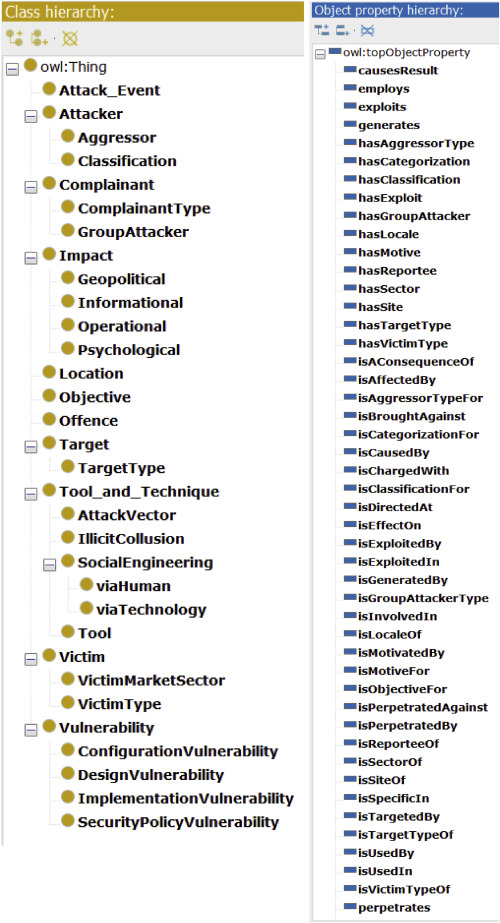
Several ontologies have been developed within the field of cybercrime, but the ontology that specifically addresses cybercrime attacks has not been previously developed. The existing ontologies in this field have been engineered for different aspects of cybercrime, such as cybercriminal profiles, legislation, or forensic investigations. We have collected all information required for ontology from Computer Information System Company (CISCO) website [1]. Finally, the use of the CyberCrime Attacks ontology will bring several benefits to the different types of individuals including:

* ***Novice Users:***To make informed decisions, implement appropriate security measures, and protect their personal information from potential threats.
* ***Students:*** Equips students with valuable knowledge and skills related to cybersecurity, digital literacy and personal protection, ethics and research.
* ***Domain Experts:*** Empowers domain experts with a structured framework, comprehensive understanding, threat intelligence analysis, training resources, and support for policy development.

1. **Related Work**

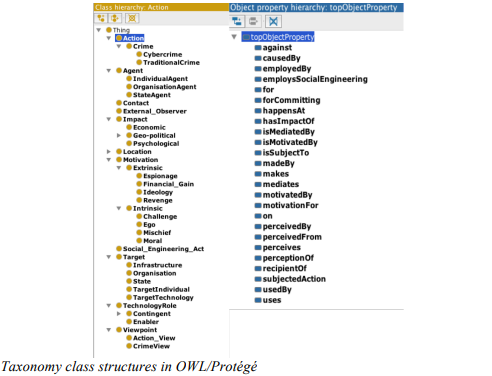
In this section, we present the ontologies relevant to the field of cybercrime that we found. Although we were unable to find any specific CyberCrime Attacks ontology that could be directly reused or re-engineered. But, the identified ontologies proved valuable in understanding an approach to develop the Cybercrime Attacks ontology. The following ontologies we found:

Toward cybercrime classification ontology: A knowledge-based approach: In recent years there has been an increase in cybercrimes and its negative impacts on the lives of individuals, organizations, and governments. It has been argued that a better understanding of cybercrime is a necessary condition to develop appropriate legal and policy responses to cybercrime. While a universally agreed-upon classification scheme would facilitate the development of such understanding and also collaborations, current classification schemes are insufficient, fragmented and often incompatible since each focuses on different perspectives (e.g., role of the computer, attack, attacker's or defender's viewpoint), or uses varying terminologies to refer to the same thing, making consistent cybercrime classifications improbable. In this paper we present and illustrate a new cybercrime ontology that incorporates multiple perspectives and offers a more holistic viewpoint for cybercrime classification than prior works. This incorporates various perspectives from different stakeholders, such as law enforcement agencies, cybersecurity experts, and legal professionals, to create a robust and inclusive understanding of cybercrime. The primary objective is to construct a cybercrime conceptual model that encompasses a set of interconnected concepts. It should therefore prove to be a more useful tool for cybercrime stakeholders [2].

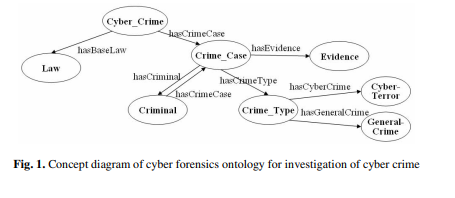


Most cybercrime classification schemes are just presented as taxonomies. An Ontological representation of a taxonomy for a cybercrime: The modern phenomenon of cybercrime raises issues and challenges on a scale that has few precedents. A particular central concern is that of establishing clarity about the conceptualization of cybercrime and its growing economic cost to society.

A further related concern is focused on developing appropriate legal and policy responses in a context where crime transcends national jurisdictions and physical boundaries. Both are predicated on a better understanding of cybercrime. Efforts at defining and classifying cybercrime by the use of taxonomies to date have largely been descriptive with resulting ambiguities. This paper contributes a semi-formal approach to the development of a taxonomy for cybercrime and offers the conceptual language and accompanying constraints with which to describe cybercrime examples. The approach uses the ontology development platform, Protégé and the Unified Modeling Language (UML) to present an initial taxonomy for cybercrime that goes beyond the descriptive accounts previously offered. The taxonomy is illustrated with examples of cybercrimes both documented in the Protégé toolset and also using UML [3].

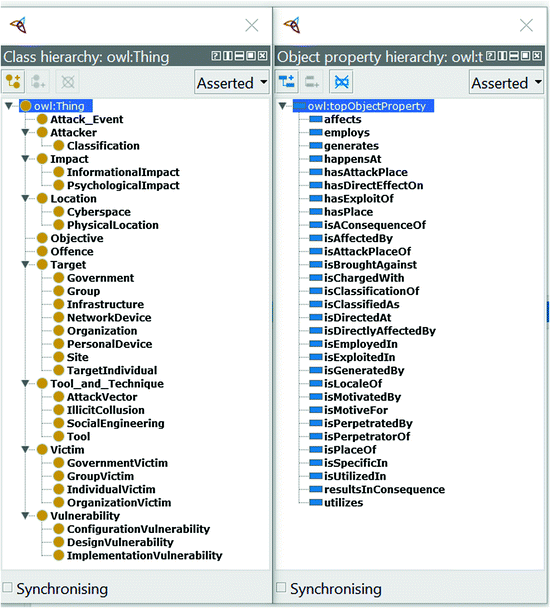


Cyber Forensics Ontology for Cyber Criminal Investigation: We developed Cyber Forensics Ontology for the criminal investigation in cyber space. Cybercrime is classified into cyber terror and general cybercrime, and those two classes are connected with each other. The investigation of cyber terror requires high technology, system environment and experts, and general cybercrime is connected with general crime by evidence from digital data and cyber space. Accordingly, it is difficult to determine relational crime types and collect evidence. Therefore, we considered the classifications of cybercrime, the collection of evidence in cyber space and the application of laws to cybercrime. In order to efficiently investigate cybercrime, it is necessary to integrate those concepts for each cybercrime-case. Thus, we constructed a forensics domain ontology for criminal investigation in cyber space, according to the categories of cybercrime, laws, evidence and information of criminals. This ontology can be used in the process of investigating of cybercrime-cases, and for data mining of cybercrime; classification, clustering, association and detection of crime types, crime cases, evidences and criminals [4].

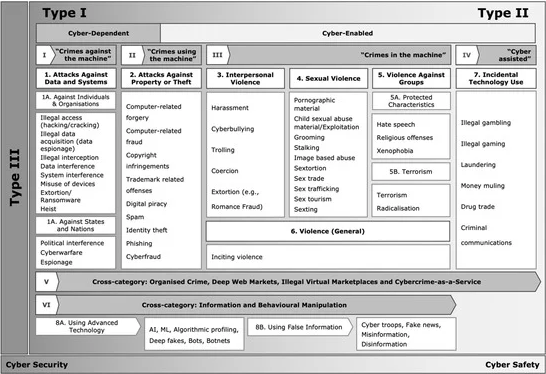


Cyber Identity: Salient Trait Ontology and Computational Framework to Aid in Solving Cybercrime: Cyber forensics is challenging due to the lack of defined holistic features with a ground truth identity core, and scalable systematic methods to credibly link a person's physical and cyber attributes in a complex networked environment. Cybercrime continues to grow as humans conduct more online activities that generate sensitive data while connected to anyone around the world. In this work, we propose a new classification-based ontology and computational framework for resolving an identity based on cyber activities. Our ontology and framework extend legal case situational theory research to temporally map cyber and physical categorical traits. Initial experimentation based on real-world legal cases reveals contextual salient traits that are most effective in linking evidence to a person's profile or unique identity. As a result, these multi-dimensional traits support innovative visualizations that depict a person's linkable identity core, digital artifacts, security, and technology. The impact of our ontology and framework design is to support solving cybercrime by aiding in identity resolution [5].

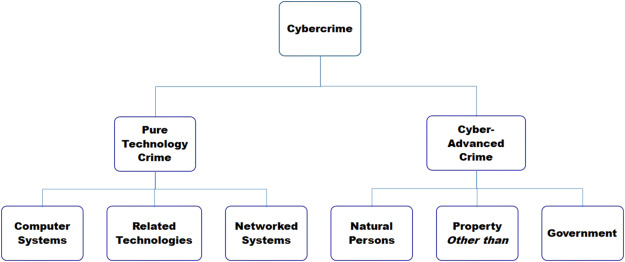
An Ontological Approach to Classifying Cybercrimes in an ICT4D Context: While the phenomenon of cybercrime remains a challenge for governments worldwide, it is even more of a challenge for countries in an ICT4D context since they possess limited technical skills and resources to respond to, investigate and prosecute nefarious cyber activities. Despite the challenges, governments have responded by establishing legal frameworks and Computer Security Incident Response Teams. However, scholars argue that the cybercrime phenomenon is still not well understood; which is compounded by the lack of an accepted, uniform cybercrime classification scheme or ontology with which to classify cybercrimes. While few classification schemes have been published, same are limited in that they are not comprehensive; i.e., they are unable to account for the range of and ever changing types of cybercrimes and, the schemes are largely incompatible, focusing on different perspectives. This makes holistic and consistent classification improbable. To address these gaps we propose a formal cybercrime classification ontology, expressed in OWL Ontology Language. In designing our ontology we were guided by the steps of the design science research methodology. This paper contributes a formal ontology of a ‘shared conceptualization’ of cybercrimes by police practitioners and researchers. The ontology presented here is improved over prior works since it incorporates multiple perspectives and its design is better able to handle existing and future cybercrimes, a most salient feature given the dynamic nature of cybercrimes. We demonstrate the ontology by applying it to an actual cybercrime case. The designed ontology classifies the cybercrime and has the potential to improve cybercrime classification in ICT4D [6].



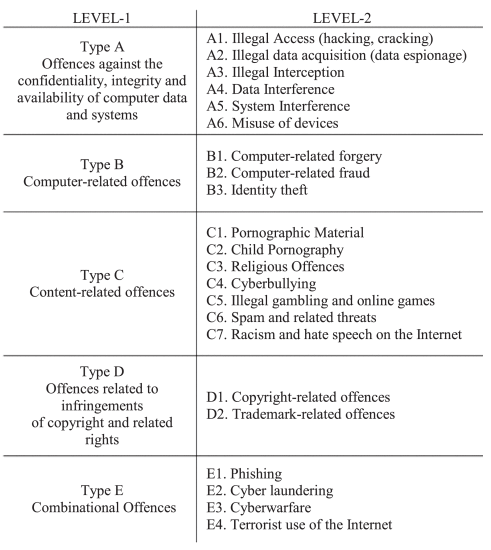
Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies: Cybercrime is becoming ever more pervasive and yet the lack of consensus surrounding what constitutes a cybercrime has a significant impact on society, legal and policy response, and academic research. Difficulties in understanding cybercrime begin with the variability in terminology and lack of consistency in cybercrime legislation across jurisdictions. In this review, using a structured literature review methodology, key cybercrime definitions, typologies and taxonomies were identified across a range of academic and non-academic (grey literature) sources. The findings of this review were consolidated and presented in the form of a new classification framework to understand cybercrime and cyber deviance. Existing definitions, typologies and taxonomies were evaluated, and key challenges were identified. Whilst conceptualizing cybercrime will likely remain a challenge, this review provides recommendations for future work to advance towards a universal understanding of cybercrime phenomena as well as a robust and comprehensive classification system [7].



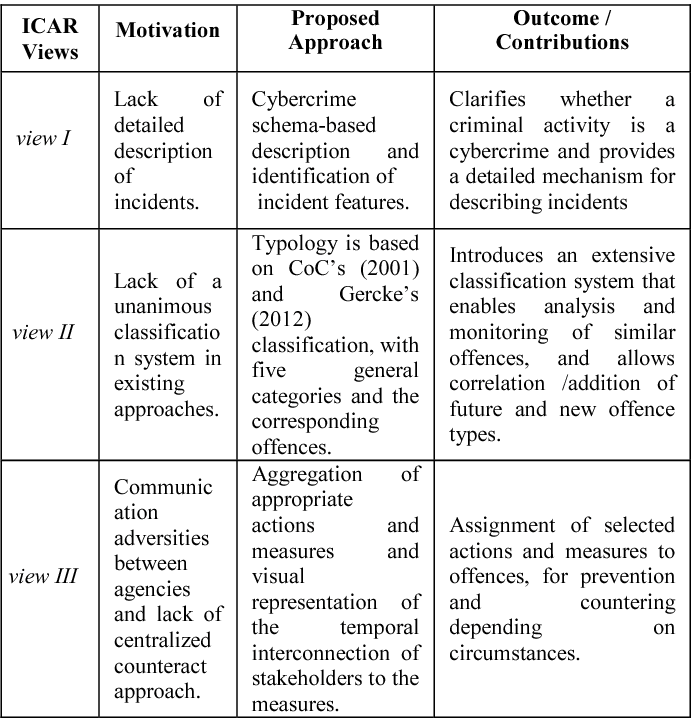
A taxonomy of cybercrime: Theory and design which develops a theory-based taxonomy for cybercrime. The need for a cybercrime taxonomy stems from the lack of a definition and standards to measure and manage cybercrime. The four building blocks of our taxonomy include mutual exclusivity, structure, exhaustiveness, and well-defined categories, which together provide the theoretical foundation [8].



A Systematic Approach toward Description and Classification of Cybercrime Incidents: 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 [9].



Cybercrime Offences: Identification, Classification and Adaptive Response: Multiple studies and surveys focus on specific cybercrime characteristics or develop classification models that do not adequately address the complexity of this contemporary type of crime. This study proposes a comprehensive approach towards cybercrime interpretation and action recommendation through a proposed framework that provides three separate and complementary views to achieve a comprehensive perspective that leads to actionable recommendations. The framework's view I identifies the features of a cybercrime incident and their corresponding elements generating a textual schema-based description that can accommodate existing and new instances of cybercrime. The second view introduces an up-to-date cybercrime-related offence classification system through consolidation and elaboration of existing approaches and leads to a visual extension of schema-based incident description that depicts the interrelations of the various cybercrime elements towards a particular type of offence. View III identifies and interconnects the relevant stakeholders with preventive and response actions and measures. The proposed framework extends previous published work on the theoretical foundation of this multi-faceted domain, and demonstrates that the necessity of a comprehensive approach towards cybercrime can be actualized through different steps with each one designated towards a different perspective [10].



Investigating Various Approaches and Ways to Detect Cybercrime: Cyber security is one of the major concepts of cyber world which provides protection to the cyberspace from various sorts of cybercrimes. This research paper provides detailed information of cybersecurity. We conduct the survey of security of recent prominent researches and categories the recent incidents in context to varied fundamental principles of cybersecurity. We have proposed a new taxonomy of cybercrime which can cover all types of cyberattacks. We have analyzed multiple cyberattacks in accordance with the updated cybercrime taxonomy to highlight the challenges in the field of cybersecurity and future research directions added in this field. In India, most of the cases are found where crimes are committed due to lack of data or by mistake. In this paper, I even have discussed various categories and cases of cybercrime which is committed thanks to lack of data or sometimes thanks to intention behind. In India also, suggested various preventive measures against these unlawful acts in day-to-day life. Now day-by-day cybercrime has increased, and criminal finds new ways of crime, use new techniques for crime completion. Here, we have mentioned techniques to solve cases. We have researched various approaches for detection of cybercrime. In this paper, we have provided the details [11].

Cyber Attacks: Detection and Prevention: Tens of millions of cyber-attacks (Emails, online transactions, live video streaming, online games, and navigation are all examples of fraudulent Internet-based intelligence gathering.) are launched every day against Internet users throughout the world. Various defences have been developed by researchers in response to these attacks. At present, the techniques that cyber attackers use to perpetrate attacks are related to human exploitation. These attacks are more frequent than before, and they are harder to contain. In the area of information management, cybersecurity is essential. In today's world, protecting privacy has been one of the most difficult tasks. "Cyber-crimes" is the first thing that has come to me when I think about cyber security, which are on the rise at an alarming rate. Various governments and corporations are taking various actions to tackle cybercrime. Despite different initiatives, cyber security remains a major issue for many people. Traditional non-confidence counter-measures are unable to prevent violations against individuals. This paper explains the current state of cybersecurity threats, counter-measures and non-confidence tools that are relevant to day-to-day online operations. It offers a valuable cyber-attack taxonomy and classification that aids in the identification of cyber-attacks and cyber-security initiatives [12].

1. **Design Methodology**

Design Methodology refers to the systematic process or sequence of steps followed to create, modify, or refine an ontology. Several methodologies have been developed to guide the ontology engineering process such as Methontology [13], On-To-Knowledge [14], NeOn [15]. Methontology is a well-known methodology that provides a structured and systematic approach to ontology engineering. It is based on the Unified Foundational Ontology (UFO) and promotes the use of a set of recommended activities and tasks. The process steps are defining ontology high level structure, developing conceptual model, transforming conceptual model into formal representation, implementation of ontology, establishing plan for maintenance.

The On-To-Knowledge methodology is designed to facilitate the development of ontologies for knowledge representation and reasoning. It focuses on knowledge acquisition and reuse. The four steps are: *Feasibility study* to determine whether to begin the actual development of the ontology. *Kickoff* where the requirements are specified and a semi-formal ontology description is developed. *Refinement* where the target ontology is obtained by refining and formalizing the semi-formal one. *Evaluation* where the evaluation of the ontology is done. *Application and evolution* where the ontology is applied in the target system and maintained. NeOn methodology presents a more comprehensive approach compared to the previous two methods. It introduces nine potential scenarios, a glossary of processes and activities, two ontology life cycle models (waterfall life cycle model, iterative-incremental life cycle model). The basic version is Four-phase model, which involves initiation, design, implementation, and maintenance stages. The methodology strongly emphasizes the significance of reusing and re-engineering both ontological and non-ontological knowledge resources. It provides detailed guidelines for conducting each activity within each phase of the ontology development process, along with recommendations for tools and techniques to support each step. We selected Neon methodology.

1. **Development**

We selected Neon methodology for our ontology development. We have examined both NeOn life cycles (Waterfall and Iterative- incremental) and selected iterative incremental life cycle.

***4.1. Initiation***

We created Ontology Requirement Specification Document that includes: purpose, scope, implementation language, functional and non-functional requirements for the CyberCrime Attacks Ontology. Functional Requirements are divided into *Competency Questions’* groups. Competency question groups are: cybercrime, mail bomb, mail spam, cryptanalysis, crypto-jacking, side channel, espionage, identity theft, sabotage, cross site scripting, DNS, session hijacking, SQL injection, IP spoofing, packet sniffers, man-in-the-middle, ARP table poisoning, IPsec flood, Ipv6 fragments, DDoS, unauthorized access, routing information protocol, traffic analysis, DHCP spoofing, smurf, TCP-SYN flood, malicious code injection, malicious node injection, physical damage, pre-texting, virus, worm, adware, spyware, root-kit, DoS, password spraying, brute-force, dictionary, key-logger, rainbow table attacks.

***4.2. Reuse***

This section incorporates both ontological and non-ontological resources that have been thoroughly researched and employed. We have taken non ontological resources from CISCO for all sections. And no resources reused in all the sections.

***4.3. Merging***

We have not merged any ontology in our ontology. We have designed our ontology from scratch.

***4.4. Re-engineering***

In order to transform the mentioned non-ontological resources into conceptual models, a re-engineering process was undertaken. This process involved analyzing the structure of each resource. Once the conceptual model for each resource was developed, they were utilized as input during the design phase.

***4.5. Design***

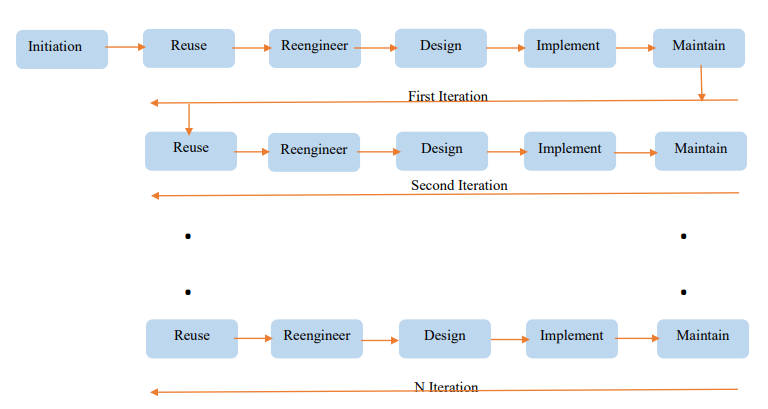
Modularization of ontologies plays a crucial role in enhancing the development, reuse, and maintenance of an ontology. It aligns with the dimensionality approach derived from the ORSD analysis. Consequently, each of the five dimensions was uniquely represented by a module: email attacks, encryption attacks, insider threat attacks, network attacks, physical attacks, social engineering attacks and software attacks.

***4.6. Implementation***

A formal model, expressed in Description Logic, was created and implemented in OWL Web Ontology Language using Protégé.

***4.7. Maintenance***

The maintenance phase is currently in progress, during which any identified errors in the ontology will be addressed. If an error is detected, the ontology will be taken back to the design phase for correction.

**

**Summary of Ontology Requirements Specification Document**

1. **Purpose**

The purpose of building ontology is to provide a knowledge model of attack types of cybercrime.

1. **Scope**

The ontology has to focus just on cybercrime attack types, not its whole domain.

1. **Implementation Language**

The ontology has to be implemented in OWL Language.

1. **Intended Users:**

|  |  |
| --- | --- |
| *User 1:* | Students |
| *User 2:* | Novice Users |
| *User 3:* | Domain Experts |

1. **Intended Uses:**

|  |  |
| --- | --- |
| Use 1: | To describe different cybercrime attacks. |
| Use 2: | To represents the information monitored by authentic sources. |
| Use 3: | To provides latest information about cybercrime attack types. |

1. **Ontology Requirements**
2. **Non-Functional Requirements**

NFR1. The ontology must provide latest information about cybercrime attack types.

NFR2. The ontology must support English Language.

1. **Functional Requirements (Competency Question Groups)**

**CQG1: Cybercrime**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Questions** | | |
| CQ1.1: | | Where first cybercrime Introduced? | |
| CQ1.2: | | | Who done the first cybercrime? |
| CQ1.3: | | | When was the first cybercrime done on? |

**CQG2: Mail Bomb Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ2.1: | What is best defense against mail bomb attack? |
| CQ2.2: | What are prevention techniques of mail bomb attack? |
| CQ2.3: | What are detection techniques of mail bomb attack? |
| CQ2.4: | What are vulnerabilities of mail bomb attack? |

**CQG3: Mail Spam Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ3.1: | What is best defense against mail spam attack? |
| CQ3.2: | What are prevention techniques of mail spam attack? |
| CQ3.3: | What are detection techniques of mail spam attack? |
| CQ3.4: | What are vulnerabilities of mail spam attack? |

**CQG4: Cryptanalysis Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ4.1: | What is best defense against cryptanalysis attack? |
| CQ4.2: | What are prevention techniques of cryptanalysis attack? |
| CQ4.3: | What are detection techniques of cryptanalysis attack? |
| CQ4.4: | What are vulnerabilities of cryptanalysis attack? |

**CQG5: Crypto-Jacking Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ5.1: | What is best defense against crypto-jacking attack? |
| CQ5.2: | What are prevention techniques of crypto-jacking attack? |
| CQ5.3: | What are detection techniques of crypto-jacking attack? |
| CQ5.4: | What are vulnerabilities of crypto-jacking attack? |

**CQG6: Side Channel Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ6.1: | What is best defense against side channel attack? |
| CQ6.2: | What are prevention techniques of side channel attack? |
| CQ6.3: | What are detection techniques of side channel attack? |
| CQ6.4: | What are vulnerabilities of side channel attack? |

**CQG7: Espionage Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ7.1: | What is best defense against espionage attack? |
| CQ7.2: | What are prevention techniques of espionage attack? |
| CQ7.3: | What are detection techniques of espionage attack? |
| CQ7.4: | What are vulnerabilities of espionage attack? |

**CQG8: Identity Theft Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ8.1: | What is best defense against identity theft attack? |
| CQ8.2: | What are prevention techniques of identity theft attack? |
| CQ8.3: | What are detection techniques of identity theft attack? |
| CQ8.4: | What are vulnerabilities of identity theft attack? |

**CQG9: Sabotage Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ9.1: | What is best defense against sabotage attack? |
| CQ9.2: | What are prevention techniques of sabotage attack? |
| CQ9.3: | What are detection techniques of sabotage attack? |
| CQ9.4: | What are vulnerabilities of sabotage attack? |

**CQG10: Cross Site Scripting Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ10.1: | What is best defense against cross site scripting attack? |
| CQ10.2: | What are prevention techniques of cross site scripting attack? |
| CQ10.3: | What are detection techniques of cross site scripting attack? |
| CQ10.4: | What are vulnerabilities of cross site scripting attack? |

**CQG11: DNS Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ11.1: | What is best defense against DNS attack? |
| CQ11.2: | What are prevention techniques of DNS attack? |
| CQ11.3: | What are detection techniques of DNS attack? |
| CQ11.4: | What are vulnerabilities of DNS attack? |

**CQG12: Session Hijacking Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ12.1: | What is best defense against session hijacking attack? |
| CQ12.2: | What are prevention techniques of session hijacking attack? |
| CQ12.3: | What are detection techniques of session hijacking attack? |
| CQ12.4: | What are vulnerabilities of session hijacking attack? |

**CQG13: SQL Injection Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ13.1: | What is best defense against SQL injection attack? |
| CQ13.2: | What are prevention techniques of SQL injection attack? |
| CQ13.3: | What are detection techniques of SQL injection attack? |
| CQ13.4: | What are vulnerabilities of SQL injection attack? |

**CQG14: IP Spoofing Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ14.1: | What is best defense against IP spoofing attack? |
| CQ14.2: | What are prevention techniques of IP spoofing attack? |
| CQ14.3: | What are detection techniques of IP spoofing attack? |
| CQ14.4: | What are vulnerabilities of IP spoofing attack? |

**CQG15: Man-In-The-Middle Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ15.1: | What is best defense against MITM attack? |
| CQ15.2: | What are prevention techniques of MITM attack? |
| CQ15.3: | What are detection techniques of MITM attack? |
| CQ15.4: | What are vulnerabilities of MITM attack? |

**CQG16: ARP Table Poisoning Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ16.1: | What is best defense against ARP table poisoning attack? |
| CQ16.2: | What are prevention techniques of ARP table poisoning attack? |
| CQ16.3: | What are detection techniques of ARP table poisoning attack? |
| CQ16.4: | What are vulnerabilities of ARP table poisoning attack? |

**CQG17: DDoS Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ17.1: | What is best defense against DDoS attack? |
| CQ17.2: | What are prevention techniques of DDoS attack? |
| CQ17.3: | What are detection techniques of DDoS attack? |
| CQ17.4: | What are vulnerabilities of DDoS attack? |

**CQG18: IPsec Flood Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ18.1: | What is best defense against IPsec flood attack? |
| CQ18.2: | What are prevention techniques of IPsec flood attack? |
| CQ18.3: | What are detection techniques of IPsec flood attack? |
| CQ18.4: | What are vulnerabilities of IPsec flood attack? |

**CQG19: IPv6 Fragment Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ19.1: | What is best defense against Ipv6 fragment attack? |
| CQ19.2: | What are prevention techniques of Ipv6 fragment attack? |
| CQ19.3: | What are detection techniques of Ipv6 fragment attack? |
| CQ19.4: | What are vulnerabilities of Ipv6 fragment attack? |

**CQG20: Packet Sniffers Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ20.1: | What is best defense against packet sniffers attack? |
| CQ20.2: | What are prevention techniques of packet sniffers attack? |
| CQ20.3: | What are detection techniques of packet sniffers attack? |
| CQ20.4: | What are vulnerabilities of packet sniffers attack? |

**CQG21: Routing Information Protocol Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ21.1: | What is best defense against routing information protocol attack? |
| CQ21.2: | What are prevention techniques of routing information protocol attack? |
| CQ21.3: | What are detection techniques of routing information protocol attack? |
| CQ21.4: | What are vulnerabilities of routing information protocol attack? |

**CQG22: Traffic Analysis Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ22.1: | What is best defense against traffic analysis attack? |
| CQ22.2: | What are prevention techniques of traffic analysis attack? |
| CQ22.3: | What are detection techniques of traffic analysis attack? |
| CQ22.4: | What are vulnerabilities of traffic analysis attack? |

**CQG23: DHCP Spoofing Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ23.1: | What is best defense against DHCP spoofing attack? |
| CQ23.2: | What are prevention techniques of DHCP spoofing attack? |
| CQ23.3: | What are detection techniques of DHCP spoofing attack? |
| CQ23.4: | What are vulnerabilities of DHCP spoofing attack? |

**CQG24: Smurf Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ24.1: | What is best defense against smurf attack? |
| CQ24.2: | What are prevention techniques of smurf attack? |
| CQ24.3: | What are detection techniques of smurf attack? |
| CQ24.4: | What are the vulnerabilities of smurf attack? |

**CQG25: TCP\_SYN Flood Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ25.1: | What is best defense against TCP Syn flood attack? |
| CQ25.2: | What are prevention techniques of TCP Syn flood attack? |
| CQ25.3: | What are detection techniques of TCP Syn flood attack? |
| CQ25.4: | What are vulnerabilities of TCP Syn flood attack? |

**CQG26: Unauthorized Access Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ26.1: | What is best defense against unauthorized access attack? |
| CQ26.2: | What are prevention techniques of unauthorized access attack? |
| CQ26.3: | What are detection techniques of unauthorized access attack? |
| CQ26.4: | What are vulnerabilities of unauthorized access attack? |

**CQG27: Malicious Code Injection Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ27.1: | What is best defense against malicious code injection attack? |
| CQ27.2: | What are prevention techniques of malicious code injection attack? |
| CQ27.3: | What are detection techniques of malicious code injection attack? |
| CQ27.4: | What are vulnerabilities of malicious code injection attack? |

**CQG28: Malicious Node Injection Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ28.1: | What is best defense against malicious node injection attack? |
| CQ28.2: | What are prevention techniques of malicious node injection attack? |
| CQ28.3: | What are detection techniques of malicious node injection attack? |
| CQ28.4: | What are vulnerabilities of malicious node injection attack? |

**CQG29: Physical Damage Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ29.1: | What is best defense against physical damage attack? |
| CQ29.2: | What are prevention techniques of physical damage attack? |
| CQ29.3: | What are detection techniques of physical damage attack? |
| CQ29.4: | What are vulnerabilities of physical damage attack? |

**CQG30: Phishing Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ30.1: | What is best defense against phishing attack? |
| CQ30.2: | What are prevention techniques of phishing attack? |
| CQ30.3: | What are detection techniques of phishing attack? |
| CQ30.4: | What are vulnerabilities of phishing attack? |

**CQG31: Pre-Texting Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ31.1: | What is best defense against whaling pre-texting attack? |
| CQ31.2: | What are prevention techniques of pre-texting attack? |
| CQ31.3: | What are detection techniques of pre-texting attack? |
| CQ31.4: | What are vulnerabilities of pre-texting attack? |

**CQG32: Adware Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ32.1: | What is best defense against adware attack? |
| CQ32.2: | What are prevention techniques of adware attack? |
| CQ32.3: | What are detection techniques of adware attack? |
| CQ32.4: | What are vulnerabilities of adware attack? |

**CQG33: DoS Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ33.1: | What is best defense against DoS attack? |
| CQ33.2: | What are prevention techniques of DoS attack? |
| CQ33.3: | What are detection techniques of DoS attack? |
| CQ33.4: | What are vulnerabilities of DoS attack? |

**CQG34: Brute-Force Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ34.1: | What is best defense against brute-force attack? |
| CQ34.2: | What are prevention techniques of brute-force attack? |
| CQ34.3: | What are detection techniques of brute-force attack? |
| CQ34.4: | What are vulnerabilities of brute-force attack? |

**CQG35: Dictionary Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ35.1: | What is best defense against dictionary attack? |
| CQ35.2: | What are prevention techniques of dictionary attack? |
| CQ35.3: | What are detection techniques of dictionary attack? |
| CQ35.4: | What are vulnerabilities of dictionary attack? |

**CQG36: Key-Logger Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ36.1: | What is best defense against key-logger attack? |
| CQ36.2: | What are prevention techniques of key-logger attack? |
| CQ36.3: | What are detection techniques of key-logger attack? |
| CQ36.4: | What are vulnerabilities of key-logger attack? |

**CQG37: Password Spraying Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ37.1: | What is best defense against password spraying attack? |
| CQ37.2: | What are prevention techniques of password spraying attack? |
| CQ37.3: | What are detection techniques of password spraying attack? |
| CQ37.4: | What are vulnerabilities of password spraying attack? |

**CQG38: Rainbow Table Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ38.1: | What is best defense against rainbow table attack? |
| CQ38.2: | What are prevention techniques of rainbow table attack? |
| CQ38.3: | What are detection techniques of rainbow table attack? |
| CQ38.4: | What are vulnerabilities of rainbow table attack? |

**CQG39: Root-Kit Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ39.1: | What is best defense against root-kit attack? |
| CQ39.2: | What are prevention techniques of root-kit attack? |
| CQ39.3: | What are detection techniques of root-kit attack? |
| CQ39.4: | What are vulnerabilities of root-kit attack? |

**CQG40: Spyware Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ40.1: | What is best defense against spyware attack? |
| CQ40.2: | What are prevention techniques of spyware attack? |
| CQ40.3: | What are detection techniques of spyware attack? |
| CQ40.4: | What are vulnerabilities of spyware attack? |

**CQG41: Virus Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ41.1: | What is best defense against virus attack? |
| CQ41.2: | What are prevention techniques of virus attack? |
| CQ41.3: | What are detection techniques of virus attack? |
| CQ41.4: | What are vulnerabilities of virus attack? |

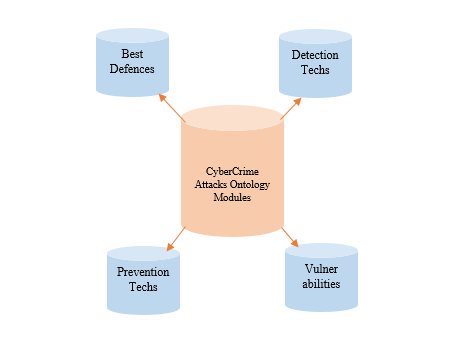
**CQG42: Worm Attacks**

|  |  |
| --- | --- |
| **ID** | **Questions** |
| CQ42.1: | What is best defense against worm attack? |
| CQ42.2: | What are prevention techniques of worm attack? |
| CQ42.3: | What are detection techniques of worm attack? |
| CQ42.4: | What are vulnerabilities of worm attack? |

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Ontology Modules**

Cybercrime attacks ontology is structured into four distinct modules, each dedicated to examining different attacks. The purpose of these modules is to offer a detailed analysis and understanding of the attacks types. These modules are as follows:



***5.1. Best Defences***

***5.1.1. Email Attacks***

Defending against email attacks is crucial to protect personal and organizational information. We can enhance email security and minimize the risk of falling victim to email attacks by using strong and unique passwords, verifying sender’s authenticity, scrutinizing the email’s content, regularly updating software, monitoring accounts and reporting suspicious activities. We described best defences against two types of email attacks which are Mail Spam and Mail Bomb. As email attacks are constantly evolving, so it's important to remain vigilant and stay updated on the latest security practices to protect yourself and your organization.

Competency questions of email attacks best defences are as follows: CQ1.1: What is best defense against mail bomb attack? CQ1.2: What is best defense against mail spam attack?

A SPARQL query to answer the competency question CQ1.1 is as follows: PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX owl: <http://www.w3.org/2002/07/owl#> PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#> PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> PREFIX smn:<https://github.com/syedamoaddatnaqvi-141/CyberCrimeOntology#> SELECT ?subject

WHERE {?subject a smn:MailBombAttacksBestDefence}

***5.1.2. Encryption Attacks***

Encryption attacks can pose a serious threat to the security of sensitive data and communication. To defend against encryption attacks effectively, it is important to implement robust security measures. Here are some best defences against encryption attacks: secure communication channels, regular updates and patching, strong access controls, security audits and penetration testing, user awareness and training, incident response and recovery. We described best defences against three types of encryption attacks which are: cryptanalysis, crypto-jacking and side channel attacks.

***5.1.3. Insider Threat Attacks***

Defending against insider threat attacks requires a multi-layered approach that combines technical controls, policies and procedures, and employee education. Here are some of the best defences against insider threat attacks: implement strong access controls, monitor and analyze user activity, data loss prevention, incident response and investigation, and strong security culture. We described best defences against three types of insider threat attacks which are: espionage, identity theft and sabotage attacks.

***5.1.4. Network Attacks***

Defending against network attacks is crucial to maintaining the security and integrity of your systems and data. Here are some essential defences against network attacks: firewalls, secure network architecture, strong authentication mechanisms, regular patching and updates, employee training and awareness, strong password policies, network monitoring and log analysis, incident response plan. We described best defences against different types of network attacks which are man-in-the-middle, packet sniffers, routing information protocols, IP spoofing, unauthorized access and traffic analysis. Additionally, we described application layer, transport layer and network layer attacks types.

***5.1.5. Physical Attacks***

Physical attacks targeting computers can have severe consequences for both individuals and organizations. When it comes to defending against physical attacks on computers, there are several measures you can take to enhance security. Here are some best practices: physical access control, surveillance and monitoring, environmental controls, regular backups and off-site storage, security awareness training. We described best defences against three types of physical attacks which are malicious code injection, malicious node injection and physical damage attacks.

***5.1.6. Social Engineering Attacks***

Defending against social engineering attacks requires a combination of awareness, education, and implementing robust security measures. Here are some of the best defences against social engineering attacks: education and awareness, regular security updates, verify requests, implement security policies, restricted access and privileges, security awareness testing, robust email filtering, continuous monitoring and logging. We described best defences against two types of social engineering attacks which are pre-texting and phishing attacks.

***5.1.7. Software Attacks***

Defending against software attacks is crucial to maintaining the security and integrity of computer systems. Here are some of the best defences against software attacks: regular software updates, firewalls, secure configuration, secure development practices, user education and awareness, encryption, antivirus and anti-malware software, multi-factor authentication. We described best defences against seven types of software attacks which are: adware, spyware, virus, worm, DoS, root-kit, password attacks and its types.

***5.2. Detection Techniques***

***5.2.1. Email Attacks***

Detecting email attacks is crucial for identifying and mitigating potential threats. Common techniques and strategies used for detecting email attacks are email filtering and spam detection, sender reputation analysis, content analysis, URL and link analysis, email authentication, user reporting and feedback and security awareness training. By employing a combination of these detection techniques, organizations can enhance their ability to identify and respond to email attacks, mitigating potential risks and minimizing the impact of successful attacks. We described detection techniques against two types of email attacks which are mail spam and mail bomb.

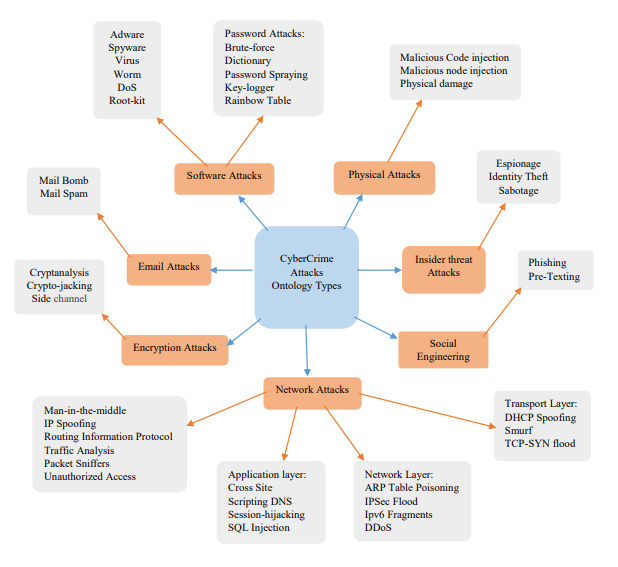
Competency questions of email attacks detection techniques are as follows: CQ1.1: What are detection techniques against mail bomb attack? CQ1.2: What are detection techniques against mail spam attack?

A SPARQL query to answer the competency question CQ1.1 is as follows: PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX owl: <http://www.w3.org/2002/07/owl#> PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#> PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> PREFIX smn:<https://github.com/syedamoaddatnaqvi-141/CyberCrimeOntology#> SELECT ?subject

WHERE { ?subject a smn:MailBombAttacksDetectionTech}

***5.2.2. Encryption Attacks***

Detecting encryption attacks can be challenging because they often aim to exploit vulnerabilities in encryption algorithms or implementation flaws. However, there are certain techniques and strategies that can help in detecting encryption attacks. Here are some common detection techniques: anomaly detection, traffic analysis, signature-based detection, log monitoring and analysis, implementing security information and event management. Detection techniques may vary depending on the specific encryption attack being targeted. We described detection techniques against three types of encryption attacks which are: cryptanalysis, crypto-jacking and side channel attacks.



***5.2.3. Insider Threat Attacks***

Detecting insider threat attacks can be challenging because insiders often have authorized access to systems and data. However, there are several techniques and indicators that can help organizations detect and identify potential insider threats. Here are some common detection techniques: user behavior analytics, log analysis, data loss prevention systems, privileged user monitoring, network traffic analysis and integration of data sources. We described detection techniques against three types of insider threat attacks which are: espionage, identity theft and sabotage attacks.

***5.2.4. Network Attacks***

Detecting network attacks is essential for identifying and mitigating threats before they cause significant damage. Here are some common techniques for detecting network attacks: intrusion detection systems, intrusion prevention systems, log analysis, network traffic analysis, honey pots, threat hunting, network segmentation and access controls and behavior analytics. We described detection techniques against different types of network attacks which are man-in-the-middle, packet sniffers, routing information protocols, IP spoofing, unauthorized access and traffic analysis. Additionally, we described application layer, transport layer and network layer attacks types.

***5.2.5. Physical Attacks***

Detecting physical attacks on computers requires a combination of technical measures and vigilance. Here are some common detection techniques: intrusion detection systems, video surveillance, tamper-evident seals, environmental monitoring sensors, access logs and auditing, physical security assessments, employee awareness and reporting. Physical attacks can be challenging to detect, especially if they are carried out by individuals with knowledge of the target systems. We described detection techniques against three types of physical attacks which are malicious code injection, malicious node injection and physical damage attacks.

***5.2.6. Social Engineering Attacks***

Detecting social engineering attacks can be challenging since they often exploit human vulnerabilities rather than technical vulnerabilities. However, there are several techniques and indicators that can help in identifying potential social engineering attempts. Here are some detection techniques for social engineering attacks: employee training and awareness, suspicious requests for information, unusual urgency or threats, unexpected or unusual communication channels, inconsistencies in communication, verification of identities, phishing email indicators, unusual network or system behavior. We described detection techniques against two types of social engineering attacks which are pre-texting and phishing attacks.

***5.2.7. Software Attacks***

Detecting software attacks is crucial for identifying and responding to security threats in a timely manner. Here are some common detection techniques used to identify software attacks: intrusion detection systems, log analysis, signature-based detection, heuristic detection, network traffic analysis, threat intelligence and honey pots. We described detection techniques against seven types of software attacks which are: adware, spyware, virus, worm, DoS, root-kit, password attacks and its types.

***5.3. Prevention Techniques***

***5.3.1. Email Attacks***

Preventing email attacks is essential to safeguard personal and organizational information. Here are some effective prevention techniques to mitigate the risk of email attacks: employee education and awareness, implement email authentication protocols, using advanced threat protection solutions, multi-factor authentication, regular backup and recovery and incident response planning. By implementing these prevention techniques, organizations can significantly reduce the likelihood of email attacks and protect sensitive information from falling into the wrong hands. We described prevention techniques against two types of email attacks which are mail spam and mail bomb.

Competency questions of email attacks prevention techniques are as follows: CQ1.1: What are prevention techniques against mail bomb attack? CQ1.2: What are prevention techniques against mail spam attack?

A SPARQL query to answer the competency question CQ1.1 is as follows: PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX owl: <http://www.w3.org/2002/07/owl#> PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#> PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> PREFIX smn:<https://github.com/syedamoaddatnaqvi-141/CyberCrimeOntology#> SELECT ?subject

WHERE { ?subject a smn:MailBombAttacksPreventionTech}

***5.3.2. Encryption Attacks***

Preventing encryption attacks is essential to ensure the security and confidentiality of sensitive data. Here are some prevention techniques to mitigate the risk of encryption attacks: using strong encryption algorithms, secure key management, two-factor authentication and network segmentation. We described prevention techniques against three types of encryption attacks which are: cryptanalysis, crypto-jacking and side channel attacks.

***5.3.3. Insider Threat Attacks***

Preventing insider threat attacks requires a proactive approach that combines various prevention techniques. Here are some effective prevention techniques to mitigate the risk of insider threats: rigorous employee screening, clear acceptable use policies, monitoring and auditing, segregation of duties, encryption and data protection. We described prevention techniques against three types of insider threat attacks which are: espionage, identity theft and sabotage attacks.

***5.3.4. Network Attacks***

Prevention is key to minimizing the risk of network attacks. Here are some effective techniques to prevent network attacks: strong perimeter defence, secure configuration management, access control and least privilege, patch management, encryption, security monitoring and incident response, regular security audits and testing. We described prevention techniques against different types of network attacks which are man-in-the-middle, packet sniffers, routing information protocols, IP spoofing, unauthorized access and traffic analysis. Additionally, we described application layer, transport layer and network layer attacks types.

***5.3.5. Physical Attacks***

Preventing physical attacks on computers requires a combination of security measures and best practices. Here are some prevention techniques: physical access control, secure physical infrastructure, regular security assessments, secure storage and disposal, incident response planning. We described detection techniques against three types of physical attacks which are malicious code injection, malicious node injection and physical damage attacks.

***5.3.6. Social Engineering Attacks***

Preventing social engineering attacks requires a proactive approach and a combination of technical measures and best practices. Here are some prevention techniques to help mitigate the risk of social engineering attacks: strong password policies and multifactor authentication, robust email security, restricted access and privileges secure network and systems, phishing simulation and testing, ongoing monitoring and updates, regular security audits and assessments. We described prevention techniques against two types of social engineering attacks which are pre-texting and phishing attacks.

***5.3.7. Software Attacks***

Preventing software attacks is crucial for maintaining the security and integrity of computer systems. Here are some prevention techniques to help mitigate the risk of software attacks: secure coding practices, input validation and sanitization, principle of least privilege, secure configuration, secure authentication, network segmentation, secure network architecture, security testing and code reviews, backup and disaster recovery, security monitoring and incident response. We described prevention techniques against seven types of software attacks which are: adware, spyware, virus, worm, DoS, root-kit, password attacks and its types.

***5.4. Vulnerabilities***

***5.4.1. Email Attacks***

Email attacks can exploit various vulnerabilities in the email infrastructure and human behavior. Here are some common vulnerabilities associated with email attacks: malicious attachments, malicious links, man-in-the-middle attacks, email client and server vulnerabilities, insider threats and lack of user awareness. We described vulnerabilities against two types of email attacks which are mail spam and mail bomb.

Competency questions of email attacks vulnerabilities are as follows: CQ1.1: What are vulnerabilities against mail bomb attack? CQ1.2: What are vulnerabilities against mail spam attack?

A SPARQL query to answer the competency question CQ1.1 is as follows: PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> PREFIX owl: <http://www.w3.org/2002/07/owl#> PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#> PREFIX xsd: <http://www.w3.org/2001/XMLSchema#> PREFIX smn:<https://github.com/syedamoaddatnaqvi-141/CyberCrimeOntology#> SELECT ?subject

WHERE { ?subject a smn:MailBombAttacksVulnerabilities}

***5.4.2. Encryption Attacks***

While encryption is a crucial security measure, it is not entirely immune to vulnerabilities. Here are some common vulnerabilities associated with encryption attacks: weak encryption algorithms, poor key management, implementation flaws, key exchange vulnerabilities and implementation backdoors. We described vulnerabilities against three types of encryption attacks which are: cryptanalysis, crypto-jacking and side channel attacks.

***5.4.3. Insider Threat Attacks***

Insider threat attacks exploit various vulnerabilities within an organization. These vulnerabilities can arise from technical, operational, and human factors. Here are some common vulnerabilities that insider threat attacks target: excessive access privileges, weak or inadequate access controls, lack of monitoring and auditing, lack of employee engagement and insider collusion. We described vulnerabilities against three types of insider threat attacks which are: espionage, identity theft and sabotage attacks.

***5.4.4. Network Attacks***

Network attacks exploit various vulnerabilities in network systems and protocols. Here are some common vulnerabilities that attackers target: weak authentication, software and firmware vulnerabilities, misconfigurations, phishing and social engineering, network sniffing, zero-day exploits and weak wireless security. We described vulnerabilities against different types of network attacks which are man-in-the-middle, packet sniffers, routing information protocols, IP spoofing, unauthorized access and traffic analysis. Additionally, we described application layer, transport layer and network layer attacks types.

***5.4.5. Physical Attacks***

Physical attacks on computers can exploit various vulnerabilities in the physical infrastructure and human factors. Here are some common vulnerabilities to be aware of: unauthorized access, tampering with hardware, theft or loss of equipment, social engineering, lack of surveillance and monitoring, inadequate physical security controls, environmental risks and lack of incident response planning. We described prevention techniques against three types of physical attacks which are malicious code injection, malicious node injection and physical damage attacks.

***5.4.6. Social Engineering Attacks***

Social engineering attacks exploit human vulnerabilities rather than technical vulnerabilities. They take advantage of people's natural inclination to trust and manipulate their emotions and behaviors. Here are some vulnerabilities commonly exploited by social engineering attacks: lack of awareness, trusting nature, emotional manipulation, lack of security awareness training, information overload, social media and online footprint. We described vulnerabilities against two types of social engineering attacks which are pre-texting and phishing attacks.

***5.4.7. Software Attacks***

Software attacks can exploit various vulnerabilities in computer systems, applications, and networks. Here are some common vulnerabilities that software attacks target: software bugs and coding errors, weak authentication and authorization, injection attacks, cross-site request forgery, remote code execution, unpatched software and outdated systems, insecure network protocols. We described vulnerabilities against seven types of software attacks which are: adware, spyware, virus, worm, DoS, root-kit, password attacks and its types.

1. **Evaluation**

# To assess the quality of the developed CyberCrime Attacks ontology, two evaluation goals has been considered: Domain coverage to see the ontology's effectiveness in representing the considered extrusion domain, and quality of modeling in terms of design and development. During the evaluation process, the Ontology was also assessed by cybersecurity analysts, data scientists and domain experts.

***6.1. Domain Coverage***

CyberCrime Attacks Ontology developed by using non-ontological resources related to different types of attacks. After that ontology assessed by three experts who provided valuable insights from different perspectives and ensured a comprehensive assessment of the ontology's quality. Cybersecurity analysts assessed the ontology from the perspective of its domain coverage. They evaluated the extent to which the ontology captured and represented the various aspects of the considered extrusion domain, including different cybercrime attack types, best defences, detection techniques, prevention techniques and vulnerabilities. Their expertise in cybersecurity and knowledge of real-world attack scenarios helped ensure that the ontology adequately covered the relevant domain. Data scientists contributed to the evaluation process by assessing the quality of the ontology's modeling. They focused on the design and development process of the ontology, evaluating its adherence to ontological principles, clarity, coherence, and logical consistency. Their expertise in data analysis, statistical modeling, and machine learning allowed them to provide valuable insights into the ontology's effectiveness and performance. Domain experts, who possess specialized knowledge and experience in the field of cybercrime, played a crucial role in evaluating the ontology from multiple perspectives. They provided feedback on the ontology's domain relevance, practical usability, and completeness. Their input helped ensure that the ontology accurately represented the real-world complexities of cybercrime and aligned with the practical needs of cybersecurity professionals.

***6.2. Quality of Modeling***

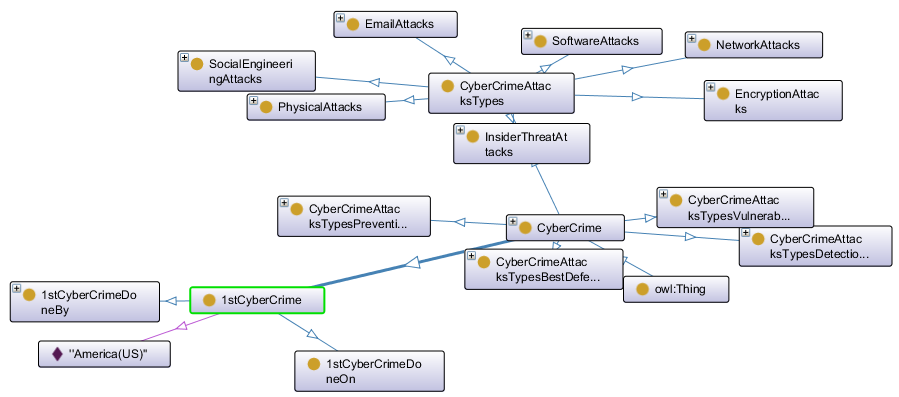
This evaluation goal centers on the ontology's quality and can be evaluated using various methods and approaches. These methods are OOPs evaluation and evaluation criteria during development process.

***6.2.1. OOPs Evaluation***

The Ontology Pitfall Scanner (OOPS!) assesses ontologies by identifying common design pitfalls found in the ontology development process. It evaluates these pitfalls based on a three-level scale: critical, important, and minor. OOPS! Is capable of semi-automatically detecting most of these pitfalls. Upon the initial evaluation of the CyberCrime Attacks Ontology, several flaws were identified and subsequently addressed and corrected.



Exploring in protégé



***6.2.2. Evaluation Criteria during Development Process***

# The criteria 16] that we have used for evaluation of the ontology during the development process are as follows:

**Accuracy:** The development process of the ontology received assistance from three experts. Additionally, the modules of the CyberCrime Attacks Ontology were created by utilizing a well-supported non-ontological resources.

**Adaptability:** Every module within the CyberCrime Attacks Ontology can be utilized independently, offering reusability and extensibility. This characteristic allows for easy adaptation of the ontology to describe various other types of cyber-attacks.

**Clarity:** The terms defined in all modules of the CyberCrime Attacks Ontology are equipped with clear and unambiguous names that enhances human readability and minimizes difficulties when creating individuals within the ontology.

**Completeness:** The CyberCrime Attacks Ontology adequately covers all the competency questions specified in the ORSD document.

**Efficiency:** The CyberCrime Attacks Ontology perform and handle computational tasks efficiently within the domain of cybercrime attacks.

**Conciseness:** The knowledge specific to the domain of cybercrime attacks has been retrieved from CISCO [1].

**Consistency:** No inconsistencies were detected in the CyberCrime Attacks Ontology during the process of reasoning.The reasoned we used HermiT 1.4.3.456.

1. **Conclusion and Future Work**

The objective of this paper is to introduce the Cybercrime Attacks Ontology, an ontology that encompasses a comprehensive set of terms to describe various forms of cyber-attacks. This ontology comprises four main modules: Best Defences, which outlines the most effective defensive measures against cyber-attacks; Detection Techniques, which covers methods for identifying and detecting cyber-attacks; Prevention Techniques, which encompasses strategies for mitigating and preventing cyber-attacks; and Vulnerabilities, which outlines the weaknesses and susceptibilities that cyber-attacks exploit. While the primary focus of the Cybercrime Attacks Ontology is on cyber-attacks, it has been designed in a manner that allows it to serve as a model for describing other types of attacks as well.

The descriptions within the Cybercrime Attacks Ontology provide an opportunity for diverse users to gain knowledge about various forms of cyber-attacks, as well as their methods of detection and prevention. The Cybercrime Attacks Ontology underwent an evaluation process focused on two key objectives: domain coverage and modeling quality. Three experts were involved in the assessment. The results of the evaluation indicate that the ontology effectively addresses the competency questions and fulfills the specified requirements. In future, we will mainly focus on those attacks that are not defined in our ontology and also cyber frameworks.

# References

# [1] <https://www.cisco.com/>

# [2] Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403-418.

# [3] Barn, R., & Barn, B. (2016). An ontological representation of a taxonomy for cybercrime.

# [4] Park, H., Cho, S., & Kwon, H. C. (2009). Cyber forensics ontology for cyber-criminal investigation. In *Forensics in Telecommunications, Information and Multimedia: Second International Conference, e-Forensics 2009, Adelaide, Australia, January 19-21, 2009, Revised Selected Papers 2* (pp. 160-165). Springer Berlin Heidelberg.

# [5] Michel, M. C., Carvalho, M., Crawford, H., & Esterline, A. C. (2018, August). Cyber identity: Salient trait ontology and computational framework to aid in solving cybercrime. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1242-1249). IEEE.

# [6] Donalds, C., & Osei-Bryson, K. M. (2018). An ontological approach to classifying cybercrimes in an ICT4D context. In *Designing for a Digital and Globalized World: 13th International Conference, DESRIST 2018, Chennai, India, June 3–6, 2018, Proceedings 13* (pp. 253-267). Springer International Publishing.

# [7] Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M.P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences.

# [8] Chandra, A., & Snowe, M.J. (2020). A taxonomy of cybercrime: Theory and design. Int. J. Account. Inf. Syst., 38, 100467.

[9] Tsakalidis, G., & Vergidis, K. (2019). A Systematic Approach toward Description and Classification of Cybercrime Incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49, 710-729.

[10] Tsakalidis, G., Vergidis, K., & Madas, M.A. (2018). Cybercrime Offences: Identification, Classification and Adaptive Response. 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), 470-475.

[11] Shah, A., & Chudasama, D. (2021). Investigating Various Approaches and Ways to Detect Cybercrime.

[12] Vakil, J., & Swaminarayan, D.P. (2022). Cyber Attacks: Detection and Prevention. International Journal of Scientific Research in Science, Engineering and Technology.

[13] <https://rhizomik.net/html/~roberto/thesis/html/Methodology.html>

[14] <https://www.researchgate.net/figure/Core-Steps-of-the-On-To-Knowledge-Methodology_fig3_220349117>

[15] <https://oeg.fi.upm.es/index.php/en/methodologies/59-neon-methodology/index.html>

[16] Vrandeciˇ c,´ Ontology Evaluation, in: Handbook on Ontologies, S. Staab and R. Studer, eds, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009, pp. 293–313. ISBN 978-3-540- 92673-3. doi:10.1007/978-3-540-92673-3\_13.