**CHAPTER 1**

**INTRODUCTION**

* 1. **Introduction About Project & Domain**

Despite the rapid escalation of cyber threats, there has still been little research into the foundations of the subject or methodologies that could serve to guide Information Systems researchers and practitioners who deal with cyber security. In addition, little is known about Crime-as-a-Service (CaaS), a criminal business model that underpins the cybercrime underground. This research gap and the practical cybercrime problems we face have motivated us to investigate the cybercrime underground economy by taking a data analytics approach from a design science perspective. To achieve this goal, we propose (1) a data analysis framework for analyzing the cybercrime underground, (2) CaaS and crime ware definitions, and (3) an associated classification model. In addition, we (4) develop an example application to demonstrate how the proposed framework and classification model could be implemented in practice. We then use this application to investigate the cybercrime underground economy by analyzing a large dataset obtained from the online hacking community. By taking a design science research approach, this study contributes to the design artifacts, foundations, and methodologies in this area. Moreover, it provides useful practical insights to practitioners by suggesting guidelines as to how governments and organizations in all industries can prepare for attacks by the cybercrime underground.

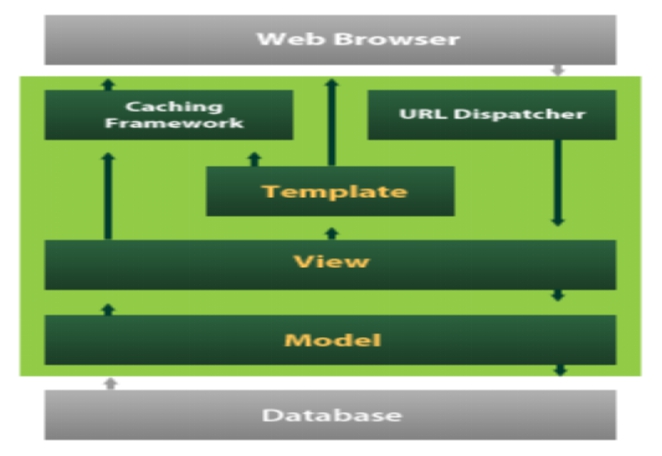
Following are the Domains for the Application:

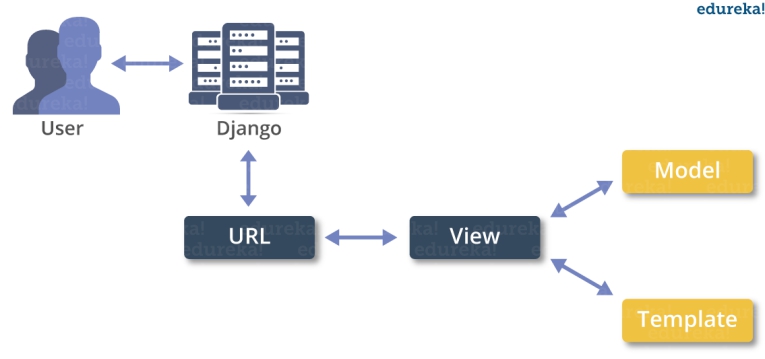
**1.PYTHON**

Python is a general-purpose interpreted, interactive, object-oriented, and high-level programming language. An [interpreted language](https://en.wikipedia.org/wiki/Interpreted_language), Python has a design philosophy that emphasizes code [readability](https://en.wikipedia.org/wiki/Readability) (notably using [whitespace](https://en.wikipedia.org/wiki/Whitespace_character) indentation to delimit [code blocks](https://en.wikipedia.org/wiki/Code_block) rather than curly brackets or keywords), and a syntax that allows programmers to express concepts in fewer [lines of code](https://en.wikipedia.org/wiki/Source_lines_of_code) than might be used in languages such as [C++](https://en.wikipedia.org/wiki/C%2B%2B)or [Java](https://en.wikipedia.org/wiki/Java_(programming_language)). It provides constructs that enable clear programming on both small and large scales. Python interpreters are available for many [operating systems](https://en.wikipedia.org/wiki/Operating_system). [CPython](https://en.wikipedia.org/wiki/CPython), the [reference implementation](https://en.wikipedia.org/wiki/Reference_implementation) of Python, is [open source](https://en.wikipedia.org/wiki/Open_source) software and has a community-based development model, as do nearly all of its variant implementations. CPython is managed by the non-profit [Python Software Foundation](https://en.wikipedia.org/wiki/Python_Software_Foundation). Python features a [dynamic type](https://en.wikipedia.org/wiki/Dynamic_type) system and automatic [memory management](https://en.wikipedia.org/wiki/Memory_management). It supports multiple [programming paradigms](https://en.wikipedia.org/wiki/Programming_paradigm), including [object-oriented](https://en.wikipedia.org/wiki/Object-oriented_programming), [imperative](https://en.wikipedia.org/wiki/Imperative_programming), [functional](https://en.wikipedia.org/wiki/Functional_programming) and [procedural](https://en.wikipedia.org/wiki/Procedural_programming), and has a large and comprehensive [standard library](https://en.wikipedia.org/wiki/Standard_library).

**2.DJANGO**

Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Web development, so you can focus on writing your app without needing to reinvent the wheel. It’s free and open source.Django's primary goal is to ease the creation of complex, database-driven websites. Django emphasizes [reusability](https://en.wikipedia.org/wiki/Reusability) and "pluggability" of components, rapid development, and the principle of [don't repeat yourself](https://en.wikipedia.org/wiki/Don%27t_repeat_yourself). Python is used throughout, even for settings files and data models.





**Figure 3.4 Django web framework**

Django also provides an optional administrative [create, read, update and delete](https://en.wikipedia.org/wiki/Create,_read,_update_and_delete) interface that is generated dynamically through [introspection](https://en.wikipedia.org/wiki/Introspection_(computer_science)) and configured via admin models

* 1. **Objective of the Project**

This project collected data from the largest hacking community and did not consider other hacking communities. Future studies will therefore need to generalize our findings by investigating a wider range of hacking communities. Second, this study has focused on the CaaS and crimeware available in the cybercrime underground, but much in-depth analysis remains to be done on the configurations of cybercrime networks.

To achieve this goal, we propose (1) a data analysis framework for analyzing the cybercrime underground,(2) CaaS and crime ware definitions, and (3) an associated classification model. In addition, we (4) develop an example application to demonstrate how the proposed framework and classification model could be implemented in practice.

We then use this application to investigate the cybercrime underground economy by analyzing a large dataset obtained from the online hacking community. By taking a design science research approach, this study contributes to the design artifacts, foundations, and methodologies in this area. Moreover, it provides useful practical insights to practitioners by suggesting guidelines as to how governments and organizations in all industries can prepare for attacks by the cybercrime underground.

Investing in cyber-threat intelligence is an important first step in understanding where high-risk vulnerabilities exist in an organisation. These are likely the same areas being targeted by mass distributed hacking platforms, and shoring up their defences can stop low-risk, high-reward threat actors before they have a chance to gain a foothold. Here the cybercrime underground has a highly professional business model that supports its own underground economy. This business model, known as CaaS(Crimeware-as-a-Service) is “a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,”. Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills.

* 1. **Existing System**

Cybercrime has undergone a revolutionary change, going from being product-oriented to service- oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world. As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation. The cybercrime underground has a highly professional business model that supports its own underground economy. This business model, known as CaaS, is “a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,”. Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills. Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds. Sood and Enbody have suggested that crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data). Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats.

* 1. **Drawbacks of Existing System**
* A previous study proposed a data mining framework for crime, dividing crimes harmful to the general public into eight categories:

1.Traffic violations. 5.Gang/Drug Offenses.

2. Sex Crime. 6. Arson.

3. Theft. 7. Violent crime.

4. Fraud. 8.Cyber-crime.

* Although this previous study explained how data mining techniques could be applied to crime analysis, it did not consider the specific features of cyber-crime.
* The “absence of capable guardians against crime” is due to organizations failing to take preventive measures against cybercrime.
* Periodic monitoring and analysis of the content of cybercrime marketplaces could help predict future cyber threats.
* Crimeware marketplaces have three key elements, namely actors (e.g., coders, operators, or buyers), value chains, and modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data).
* Consequently, the CaaS business model can involve the following roles:

1. writing a hacking program
2. performing an attack
3. commissioning an attack
4. providing an attack server (infrastructure) and laundering the proceeds.
   1. **Proposed System**

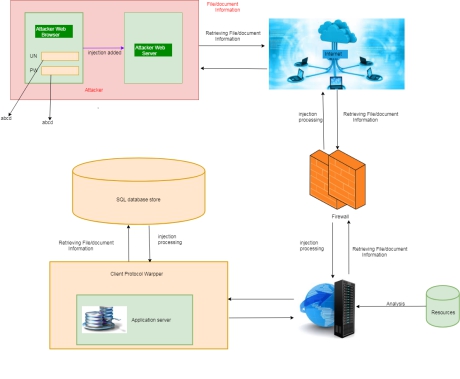
The goal of our data analysis framework is to conduct a big-picture investigation of the cybercrime underground by covering all phases of data analysis from the beginning to the end. This framework comprises four steps: (1) defining goals; (2) identifying sources; (3) selecting analytical methods; and (4) implementing an application. Because this study emphasizes the importance of RAT for analyzing the cybercrime underground, the proposed RAT-based definitions are critical to this framework: **Steps 1–2** all contain the RAT elements

A.**Step 1:** Defining Goals The first step is to identify the conceptual scope of the analysis. Specifically, this step identifies the analysis context, namely the objectives and goals. To gain an in-depth understanding of the current CaaS research, we investigated the cybercrime underground, which operates as a closed community. Thus, the goal of the proposed framework is to “investigate the cybercrime underground economy.”

B.**Step 2**: Identifying Sources the second step is to identify the data sources, based on the goals defined by Step 1. This step should consider what data is needed and where it can be obtained. Since the goal of this study is to investigate the cybercrime underground, we consider data on the cybercrime underground community. We therefore collected such data from the community itself and obtained a malware database from a leading global cyber security research firm. Because cybercriminals often change their IP addresses and use anti-crawling scripts to conceal their communications, we used a self-developed crawler that can resolve captcha’s and anti-crawling scripts to gather the necessary data. We collected a total of 2,672,091 posts selling CaaS or crimeware, made between August 2008 and October 2017, from a large hacking community site (www.hackforums.net) with over 578,000 members and more than 40 million posts.

We also collected 16,172 user profiles of sellers and potential buyers, based on their communication histories, as well as prices and questions and answers about the transactions. The black market uses traditional forum threads (e.g., bulletin boards) instead of typical e-commerce platforms (e.g., eBay, and Amazon). For example, sellers create threads in marketplace forums to sell items, and potential buyers comment on these threads. One of the most significant challenges was therefore converting this unstructured data into structured data.

**Implementation of Proposed System:**



**Figure 1.5 Implementation of Proposed System**

* Implementation is one of the critical stages of the project; it is nothing but a change of working system from the theoretical system design.
* The attacker injects payload in website database by submitting a vulnerable form with some malicious JavaScript. The victim browser page loads with the payload that has been injected as a part of the HTML body. The script will send the victims cookie to the attacker’s server.
* The attacker will now extract the victim’s cookie when the request arrives to the server. Here Java Script allows the attacker to use malicious scripts to hack important details.
* The victim will not be directly targeted by the attacker. Instead he delivers malicious java scripts while the user visits the website. Here when the attacker injects the malicious java scripts via login page.
* He will be directly allowed to access the database of our website where he can get all important information he needed.
* Finally the user can use the victim’s stolen cookies.
  1. **Advantages of Proposed System**
* Compelling and relevant content will grab the attention of potential customers and increase brand visibility.
* You can respond instantly to industry developments and be seen as ‘thought leader’ or expert in your field.
* This can improve how your business is seen by your audience.
* Positive feedback is public and can be persuasive to other potential customers.
* Negative feedback highlights areas where you can improve.
* Data mining is a technique used to mine out patterns of useful data from large data sets**.**
* The goal of the proposed framework is to “investigate the cybercrime underground economy.” This Crimeware marketplaces have three key elements, namely

1.actors (e.g., coders, operators, or buyers),

2.value chains, and

3.modes of operation (e.g., CaaS, pay-per-install, crimeware toolkits, brokerage, or supplying data).

* 1. **Project Scope & Motivation**

These proposed sets of definitions for different types of CaaS the most common account hacking methods are phishing and brute force attacks. With an emphasis on selling this as a service, we define an account hacking service as a service that offers to gain unauthorized access to a target’s account by obtaining account information (e.g., username and password) or extra security information (e.g., security questions and answers).

**Phishing Services**: The term “phishing” is a portmanteau of “password” and “fishing,” where the latter refers to catching fish using bait or a lure. We thus define a phishing service as a service that hacks accounts by pretending to be a reliable source, such as a bank or card service.

**Brute Force Attack Services**: An attacker may try to log in using one of the system’s default usernames (e.g., “root” or “admin”) by systematically trying all possible passwords. We thus define a brute force attack service as a service that hacks accounts by trying all possible passwords.

**DDoS Attack Services**: In the research literature, a DDoS attack is defined as “an attack which makes resources unavailable to its legitimate users,”. In the business practice literature, it is defined as “an attack involving an enormous number of spurious requests from a large number of computers worldwide that flood a target server,” We thus define DDoS attack service as a service that makes one target service unavailable by flooding it with traffic from multiple compromised sources.

**Spamming Services**: Over the last decade, spamming has been defined in a variety of ways in the literature. The academic literature defines spam as “unsolicited and unwanted e-mail from a stranger that is sent in bulk to large mailing lists, usually with some commercial objective,”

**Crypting Services**: Crypter encrypt programs or source code to avoid detection and tracking and thus bypass anti-virus software . Like other hacking services, encryption is sold as a service because crypters require a certain level of skill to use. The goal of such a service is to neutralize the preventive measures put in place by organizations and anti-virus software, preventing hacking programs from being caught or allowing them to be left behind to collect information. We define an crypting service as a service that encrypts malicious code by using a crypter to bypass anti-virus software.

**1.8 Organization of Report**

This chapter summarizes introduction of project which is elaborately described in later section of report, so the second chapter provides a detailed survey about this projected system which constitutes various paper related to how the performance of Python/Django can be improved. In the third chapter the requirements, constraints listed by the user for designing this application is described and following chapter illustrates design of the application which comprises of sequence diagram, architecture, and so on. Fifth chapter gives insight on implementation part and then testing techniques and test cases used for verifying this application is depicted in chapter six. Analysis of report containing snapshots is present in seventh chapter and finally conclusion and future enhancement is specified in the end.

**CHAPTER 2**

**LITERATURE SYRVEY**

**2.1 Literature Review**

# Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented because the fact it operates in the virtual world, with different spatial and temporal constraints, differentiates it from other crime taking place in the physical world As part of this change, the cybercrime underground has emerged as a secret cybercrime marketplace because emerging technological changes have provided organized cybercriminal groups with unprecedented opportunities for exploitation The cybercrime underground has a highly professional business model that supports its own underground economy. This business model, known as CaaS, is “a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes, such as attacks, infections, and money laundering in an automated manner,” .

# Thus, CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself product. Because CaaS is designed for novices, its customers do not need to run a hacking server or have high-level hacking skills. Consequently, the CaaS business model can involve the following roles: writing a hacking program, performing an attack, commissioning an attack, providing an attack server (infrastructure), and laundering the proceeds.

According to this theory, three elements are necessary for crimes to be committed:

1. a likely offender,
2. a suitable target, and
3. the absence of capable guardians against crime.

In a cybercrime context, the “likely offenders” are motivated sellers and potential buyers in the underground market, and the “suitable targets” are the targeted vulnerable organizations. The “absence of capable guardians against crime” is due to organizations failing to take preventive measures against cybercrime. Two types of product or service are available in the cybercrime underground. The first can be either CaaS or crimeware that are related to attack strategy, for example, phishing, brute force, or DDoS attacks, or can be used for spamming or creating botnets, exploits, ransomware, rootkits, or Trojans. Attack strategies often exploit system vulnerabilities such as application loopholes. In addition, social engineering attacks exploit human vulnerabilities . The most well-known example of such an attack is the use of a “secret question” for password recovery: attackers check into the user’s background to guess the secret question and hence steal the account. Examples include encryption and virtual private network (VPN) services, crypters, and proxies. From the perspective of RAT, the likely offenders are attackers motivated to attack organizations or products that constitute a suitable target. If such targets are attacked, however, both the targets and those who supply their cybersecurity products become aware of the vulnerabilities that made the attack possible, leading them to apply security updates to their software. These updates can be seen as capable guardians against crime, and the preventive measures taken can be identified by looking through each program’s version history. However, this is not the end of the matter, because the attackers will then develop and sell new versions of their hacking tools to combat the guardians, thus re-establishing the third RAT condition, the absence of capable guardians against crime. Such events can also be identified by the version numbers of the hacking tools sold on the black market: since it is an online marketplace, attackers must give detailed explanations to retain their customers’ confidence.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sl no** | **Paper Title & Year of Publication** | **Publication name** | **Findings of Proposed System (Implemented)** | **Implementation,Algorithm and methodology used** | **Remarks(Not yet implemented)** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |

**Table 2.1 Literature Review**

**Comparative analysis:**

For a number of years, policy-makers at the highest levels have been expressing their concerns that insecure information systems threaten economic growth and national security. As a result of theseconcerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. A recent publication offers a compilation and analysis of cybersecurity efforts in fourteen countries.76 The International CIIP Handbook provides an overview of issues of high importance inthe field of critical information infrastructure protection (CIIP), serves as a reference work for the interested community, and provides a basis for further research by compiling relevant material. In this chapter, the main findings of this volume are presented. We are focusing mainly on five focal points of high importance that emerged from a cross-comparison of country surveys:

**1.** **Critical Sectors**: This section compares critical infrastructure sectors as identified by the respective countries. To look at the concept of critical infrastructures is important, because ybersecurity has emerged in parallel to CIP in all countries.

**2.** **Organizational Overview**: The second part of this chapter provides an overview of important public actors in the national cybersecurity organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are not taken into account.

**3.** **Early Warning Approaches**: The third section describes national organizations responsible for cyber-early warning, namely cybersecurity-related information-sharing organizations such asCERTs (Computer Emergency Response Teams), ISACs (Information Sharing and Analysis Centers), etc.

**4.** **Current Topics in Law and Legislation:** The development of effective regulations, laws, and criminal justice mechanisms is essential in deterring virtual abuse and other offences against the information infrastructure. Moreover, a strict regulation may create trust in the new ICT and encourage the private sector and individuals to make better use of e-Commerce or e-Government services.

**5.** **Research and Development**: The last section gives an overview of recent efforts in Research and Development (R&D) concerning cybersecurity.

**2.2 Conclusion of Review**

The data analysis step of the proposed framework involves four steps. Here, we report the data analysis results: CaaS and crimeware classification and market trends, cybercrime market dynamics, and potential hacking targets.

**CaaS and Crimeware Classification and Market Trends**

Here, we evaluate the accuracy of the proposed classifications. Specifically, we analyze the CaaS and crimeware trends between 2008 and October 2017 based on these classifications. the most common classes overall were botnets (17%) and exploits (17%). The most popular classes in 2017 were botnets (33%), VPN services (20%), exploits (13%), and brute force attack services (7%). To validate our classification model, we used a confusion matrix, a common method of calculating classifier output accuracy. The training and testing datasets comprised 300 and 700 items, respectively. This gave an accuracy of 82.6% with a 95% confidence interval of (70.74%, 81.24%) for identifying the risks posed by CaaS- and crimeware related messages.

**CHAPTER 3**

**SOFTWARE REQUIREMENTS SPECIFICATION**

**3.1 Introduction**

A **Software Requirements Specification (SRS)** is a document that describes the nature of a project, software or application. In simple words, SRS document is a manual of a project provided it is prepared before you kick-start a project/application. This document is also known by the names SRS report, software document. A software document is primarily prepared for a project, software or any kind of application.There are a set of guidelines to be followed while preparing the software requirement specification document. This includes the purpose, scope, functional and nonfunctional requirements, software and hardware requirements of the project. In addition to this, it also contains the information about environmental conditions required, safety and security requirements, software quality attributes of the project etc.

The system requirement and specification of our project is as follows:

**SOFTWARE SPECIFICATIONS**

* Operating system : Windows 10
* Front End : HTML5, CSS3, JavaScript,Bootstraps
* Coding Language : Python
* Database : MySQL/Sqlite3
* Tool : Pycharm IDE
* Framework : Django web frameworks

**HARDWARE SPECIFICATIONS**

* Processor        : Intel i3 2.4 GHz
* Hard Disk   : Min 40 GB
* RAM           : 4GB or above

**3.2 Purpose of the requirements document:**

A requirements document is a document containing all the requirements to a certain product. It is written to allow people to understand *what* a product should do. Purpose and ((scope, from both a technical and business perspective. Product overview and use cases Requirements, including functional requirements (e.g. what a product should do) usability requirements technical requirements (e.g. security, network, platform, integration, client) environmental requirements support requirements interaction requirements (e.g. how the product should work with other systems) Assumptions Constraints Dependencies.

**3.3 Project Perspective:**

The project involved analyzing the design of few applications so as to make the application more users friendly. To do so, it was really important to keep the navigations from one screen to the other well ordered and at the same time reducing the amount of typing the user needs to do. In order to make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

**3.4 Functional Requirements:**

Functional requirements are used for expressing the behavior of a project, purpose and role each component. This is represented as using inputs, outputs and its behavior based on the specified input. While implementing design phase of system, functional requirements are considered and behavior of the whole project is realized using the use cases. The use case depicts the behavior, relationship between the components or modules of the project and the use case explanation for this project is illustrated in system design chapter.

* Graphical User Interface with the User.
* Admin Interface.
* Upload/Dowload Modules.
* Chat Modules.

**3.5 Non-Functional Requirements:**

**3.5.1 Practicality**

Project practicality is where you use only what is viewed as least needed to meet your goals.A communication system like tis needs hundreds of thousands of users to survive and thrive. Therefore, it should be designed to support large numbers of users, e.g., a substantial percent of a town or a campus.

**3.5.2 Efficiency**

Efficiency measures how well and productively a manger uses his resources to achieve goals. Project management places heavy focus on how to acquire the right project team to perform project tasks and to close project successfully within the agreed constraints.

**3.5.3 Cost**

Cost management is concerned with the process of planning and controlling the budget of a project or business. It includes activities such as planning, estimating, budgeting, financing, funding, managing, and controlling costs so that the project can be completed within the approved budget. Cost management covers the full life cycle of a project from the initial planning phase towards measuring the actual cost performance and project completion.

**3.5.4 Flexibility**

The need for flexibility is to deal with changed circumstances. Flexibility is used to scale back activities needing less effort while diverting resources to areas with unexpected problems.

**3.5.5 Modularity**

Modularity refers to the concept of making multiple modules first and then linking and combining them to form a complete system. Modularity enables re-usability and minimizes duplication. In addition to re-usability, modularity also makes it easierto fix problems as bugs can be traced to specific system modules, thus limiting the scope of detailed error searching.

**3.5.6 Extensibility**

Extensibility is a software engineering and systems design principle where the implementation takes future growth into consideration. The term extensibility can also be seen as a systemic measure of the ability to extend a systemand the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality.

**3.5.7 Reliability**

Reliability refers to the probability and or the likelihood that a given product will perform in the way and or manner it was intended to perform in the efforts that have been deemed required of that given product within or under a specific period of time required.

**3.5.8 Maintainability**

It is the probability that a system or system element can be repaired in a defined environment within a specified period of time. Increased maintainability implies shorter repair times.

**3.5.9 Portability**

It is a measure of how easily an application can be transferred from one computer environment to another. A computer software application is considered portable to a new environment if the effort required to adapt it to the new environment is within reasonable limits. The phrase "to port" means to modify software and make it adaptable to work on a different computer system.

**Software Requirements Specification (SRS) Table**

In this CHAPTER we specifically give a brief about Requirement Traceability Matrix which is mainly to check whether the requirements are satisfied or not.

|  |  |  |  |
| --- | --- | --- | --- |
| **Serial No.** | **Requirements**  **ID** | **Requirement**  **In Brief** | **Requirement Description** |
| 1 | RID1 | **Administrator** | admin is an business entiry, person to maintain the entire system. |
| 2 | RID2 | **Users** | Users is the one who visits the application and can access the basic information. |
| 3 | RID3 | **System Maintainers**  **(Registered User)** | System Maintainer is the service receiver |
| 4 | RID4 | **Home Page** | When we run the application we get the application home page. |
| 5 | RID5 | **Login Module** | User of the system gets login using the credentials (id an password). |
| 6 | RID6 | **Dataset** | In this module we collect opinion dataset from the reputed websites |
| 7 | RID7 | **Data Mining** | Process of analysing the data from different perspective and summarize it into useful information. |
| 8 | RID8 | **Machine Learning** | Used to develop softwares, microsoft technology more developer friendly. |
| 9 | RID9 | **Django, Pycharm** | Used to develop browser based application. |
| 10 | RID10 | **Python** | More Suitable programming langauage for real time projects. |
| 11 | RID11 | **MYSQL Server** | Microsoft technology used to store the data (opinions data) |
| 12 | RID12 | **Browsers** | IE, Google Chrome, Firefox |

**Table 3.6 SRS table**

**CHAPTER 4**

**SYSTEM DESIGN**

**System design** is a substanially important phase in project building and creation stages of whole development cycle. The system design is a mecahnsim for depicting and representing the overall architecture of the system, interfaces between the different components, the methods and parameters defined for each module and data for a system according to requirements specified by the user. In order to design a system, first step is to collect the system requirements, functional and non functional requirements , constaraints from the user. Second step is designing the system in an abstract manner, this step provides outline of all major components that is required for designing sytem architecture. Third step is detecting and addressing bottlecks generated in the abstarct or high-level design due to violation of some constarints specified by the user. Next operation is designing system in more elaborate and detailed manner and this step constitutes specifying the methods, parameters, interfaces to application components.

**4.1 High Level Diagram**

High level design reveals an abstract layout of entire application where abstract HLD pictorially depicts primitive constituents of system to be developed. The architecture of the system, the diagrams depicting flow of realtionship, flow of data are all considered as the high level designs and these designs are written using non-technical terms with slight additional technical terms.

**4.1.1 System Architecture**

System Architecture Architecture of application projects a blueprint of entire system in pictorial illustration. In this project the architecture three major components: Upload ,Download and User Chat as shown in the figure 4.1. When the user submits a batch of jobs to the system, first its sent to job-assigner c. This component in turn contains two sub components slot scheduler and workload estimator. Integral component workload estimator repeatedly collects the execution time technicalities of latterly completed tasks at periodic intervals and then this value is used for reckoning current map-reduce tasks at hand. After this second integral part, slot scheduler based on these estimation adjusts and assigns the slot ratio to map and reduce slave nodes .

A close up of a map

Description automatically generated

Figure 4.1 System Architecture

**4.2 Low Level Design**

Low level design is used describing major components of system in detail and elaborate manner so this technique is also called detailed-design. In this technique the diagram is constructed by iteratively refining the given details, requirements and constraints and also depicts modules, their parameters, methods and relationship among them.

**4.2.1 Flow Chart**

**4.2.2 Sequence Diagram**

**4.2.3 Use Case Diagram**

**4.2.4 Activity Diagram**

**CHAPTER 5**

**IMPLEMENTATION**

**5.1 System Implementation**

**5.2 Language Used for Implementation**

**5.3 Algorithm**

**5.4 Modules**

**5.5 Snapshot of Code Snippet**

**CHAPTER 6**

**TESTING**

**6.1 Testing Types**

**6.2 Test Cases**

**CHAPTER 7**

**RESULT ANALYSIS**

**7.1 Snapshot with Description**

**CONCLUSION**

This study contributes to the DSR literature in a broader IS context in several ways. Because it takes a DSR approach, it contributes to the design artifacts, foundations, and methodologies in this area. First, by creating example front-end applications, we have demonstrated how our design artifacts (the proposed framework and classification model) can be implemented in practice. Because this study takes a DSR approach, we have focused mainly on building and evaluating artifacts rather than on developing and justifying theory: “Actions are usually considered to be the main focus of behavioral science”. We have therefore proposed two artifacts: a data analysis framework and a classification model. We have also conducted an ex-ante evaluation of our classification model’s accuracy and an ex-post evaluation of its implementation using example applications. In line with the initiation perspective of DSR, these four example applications demonstrate the range of potential practical applications available to future researchers and practitioners.

Unlike previous studies that have presented general discussions of a broad range of cybercrime; our study has focused primarily on CaaS and crime ware from an RAT perspective. We have also proposed sets of definitions for different types of CaaS (phishing, brute force attack, DDoS attack, and spamming, crypting, and VPN services) and crime ware (drive-by download, botnets, exploits, ransomware, rootkits, Trojans, crypters, and proxies) based on definitions taken from both the academic and business practice literature. Based on these, we have built an RAT-based classification model. This study emphasizes the importance of RAT for investigating the cybercrime underground, so these RAT-based definitions are critically important parts of our framework.

In addition, unlike prior research that discussed the cybercrime underground economy without attempting to analyze the data, we have analyzed large- scale datasets obtained from the underground community. Looking at the CaaS and crimeware trends, our results show that the prevalence of botnets (attack-related crimeware) and VPNs has increased in 2017.This indicates that attackers consider both the preventive measures taken by organizations and their vulnerabilities. The most common potential target organizations are technology companies (28%), followed by content (22%), finance (20%), e-commerce (12%), and telecommunication (10%) companies. This indicates that a wide variety of companies in a range of industries are becoming potential targets for attackers, having become more vulnerable due to their greater reliance on technology.

**FUTURE WORK**

Although our study has made several significant findings, it nevertheless has several limitations that will need to be addressed in future studies. These will be able to add more analysis and significant further insights.

**First,** we only collected data from the largest hacking community and did not consider other hacking communities. Future studies will therefore need to generalize our findings by investigating a wider range of hacking communities.

**Second,** this study has focused on the CaaS and crimeware available in the cybercrime underground, but much in-depth analysis remains to be done on the configurations of cybercrime networks. Future research could cluster keywords and threats by industry to provide a deeper understanding of the potential vulnerabilities, and it could attempt to discover the network effects involved or the leaders of the cybercrime underground.

## Implications for Research :

This study contributes to the DSR literature in a broader IS context in several ways. Because it takes a DSR approach, it contributes to the design artifacts, foundations, and methodologies in this area [6]– [8]. First, by creating example front-end applications, we have demonstrated how our design artifacts (the proposed framework and classification model) can be implemented in practice. Despite the rapidly growing threat from cybercrime, there has been little research into practical frameworks for future cybersecurity researchers: the previous studies have not attempted to analyze the data or take a systematic modeling approach [3], [58]–[62]. In DSR, we must demonstrate that the artifacts can be implemented in a business environment for them to qualify as solving an important unsolved problem [7]. We have therefore provided an implementable framework, not just a conceptual one.

## Implications for Practice :

From a RAT perspective, the practical implications of this study mainly affect the capable guardians against crime, because our results indicate how underground attackers perceive preventive measures. A previous review of the current status of legal, organizational, and technological efforts to combat cybercrime in different countries relied on a case study of the work being done in Taiwan [64]. It made four recommendations for governments, lawmakers, international organizations, intelligence and law enforcement agencies, and researchers:

1. regularly update existing laws;
2. enhance specialized task forces;
3. use civil resources; and
4. promote cybercrime research.

The practical implications of our study are based on those of the previous study [64]. We have already discussed the fourth recommendation (“promote cybercrime research”) in the previous section, so we will now focus on the other three areas.

**First,** our study has implications for governments and lawmakers in that it recommends existing laws be regularly updated. The proposed CaaS and crimeware definitions and classification model may improve national defense and security by suggesting potential government roles and the adoption of particular regulatory policies.

**Second**, the proposed data analysis framework can be used to enhance specialized task forces. This study suggests that organizations in all industries should attempt to gain a deeper understanding of the nature of the cybercrime underground.

For example, they should be aware that there are cybercrime underground markets where hacking tools are sold.

**Third,** this study calls for researchers, companies, antivirus vendors, and governments to collaborate in the fight against cybercrime using civil resources. Rather than acting alone, these groups should unite to maximize their efficiency and effectiveness.

**Finally,** this study also has important implications for society. Over the last few years, the world has been facing cyber terrorism and cyberwar threats from nation-sponsored attackers [70]. Pollitt [71] defined cyber terrorism as “the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents.” Unlike most cybercrime, which is primarily motivated by monetary gain [72], cyber terrorists are politically motivated. As a result, governments should, for example, strengthen their ability to protect their citizens in online virtual environments by enhancing their immediate responses to threats such as cyber espionage and cyber terrorism.

**REFERENCES**

**BIBILOGRAPHY**

1. “FACT SHEET: Cybersecurity National Action Plan,” ed: The White House, 2016.
2. A. K. Sood and R. J. Enbody, “Crimeware-as-a-service—A survey of commoditized crimeware in the underground market,” Int. J. Crit. Infr. Prot., vol. 6, no. 1, pp. 28–38, 2013.

[3] S. W. Brenner, “Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships,” N. C. J. Law & Technol., vol. 4, no. 1, pp. 1-50, 2002.

[4] K. Hughes, “Entering the world-wide web,” ACM SIGWEB Newsl., vol. 3, no.1, pp. 4–8, 1994.

[5] S. Gregor and A. R. Hevner, “Positioning and Presenting Design Science Research for Maximum Impact,” MIS Quart., vol. 37, no. 2, pp. 337-356, 2013.

[6] V. G. Tasiopoulos and S. K. Katsikas, “Bypassing Antivirus Detection with Encryption,” in Proc., 18th Panhellenic Conf. on Informatics - PCI '14, New York, New York, USA, 2014, pp. 1–2: ACM Press.

[7] R. Venkateswaran, “Virtual private networks,” IEEE Potentials, vol. 20, no. 1, pp. 11–15, 2001. [9]A. K. Sood, S. Zeadally, and R. Bansal. “Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels,” IEEE Commun. Mag., vol. 55, no. 7, pp. 22– 28.2017.

[8] Z. Shi, G. M. Lee, and A. B. Whinston, “Toward a Better Measure of Business Proximity: Topic Modeling for Industry Intelligence,” MIS Quart., vol. 40, no. 4, pp. 1035–1056, 2016.

[9] A. Majchrzak and S. L. Jarvenpaa, “Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals,” J. Manag. Inf. Syst., vol. 27, no. 2, pp. 55–86, 2010.

[10] G. Giacomello, “Close to the Edge: Cyberterrorism Today,” in Understanding Terrorism, Emerald Group Publishing Limited, 2014, pp. 217–236. M. M. Pollitt, “Cyberterrorism — Fact or Fancy?,” Comput. Fraud Security, vol. 1998, no. 2, pp. 8–10, 1998.