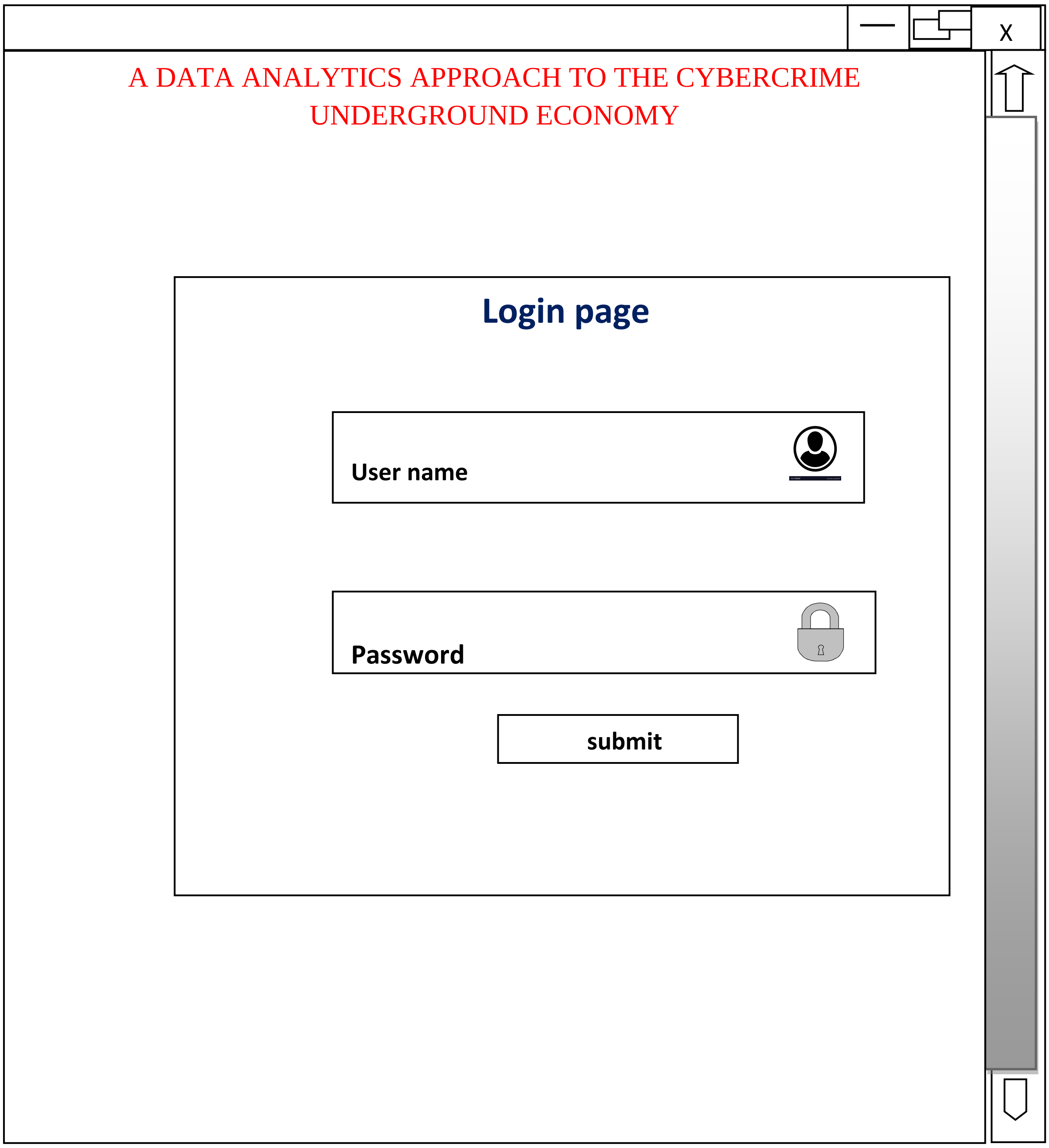
Chapter 7

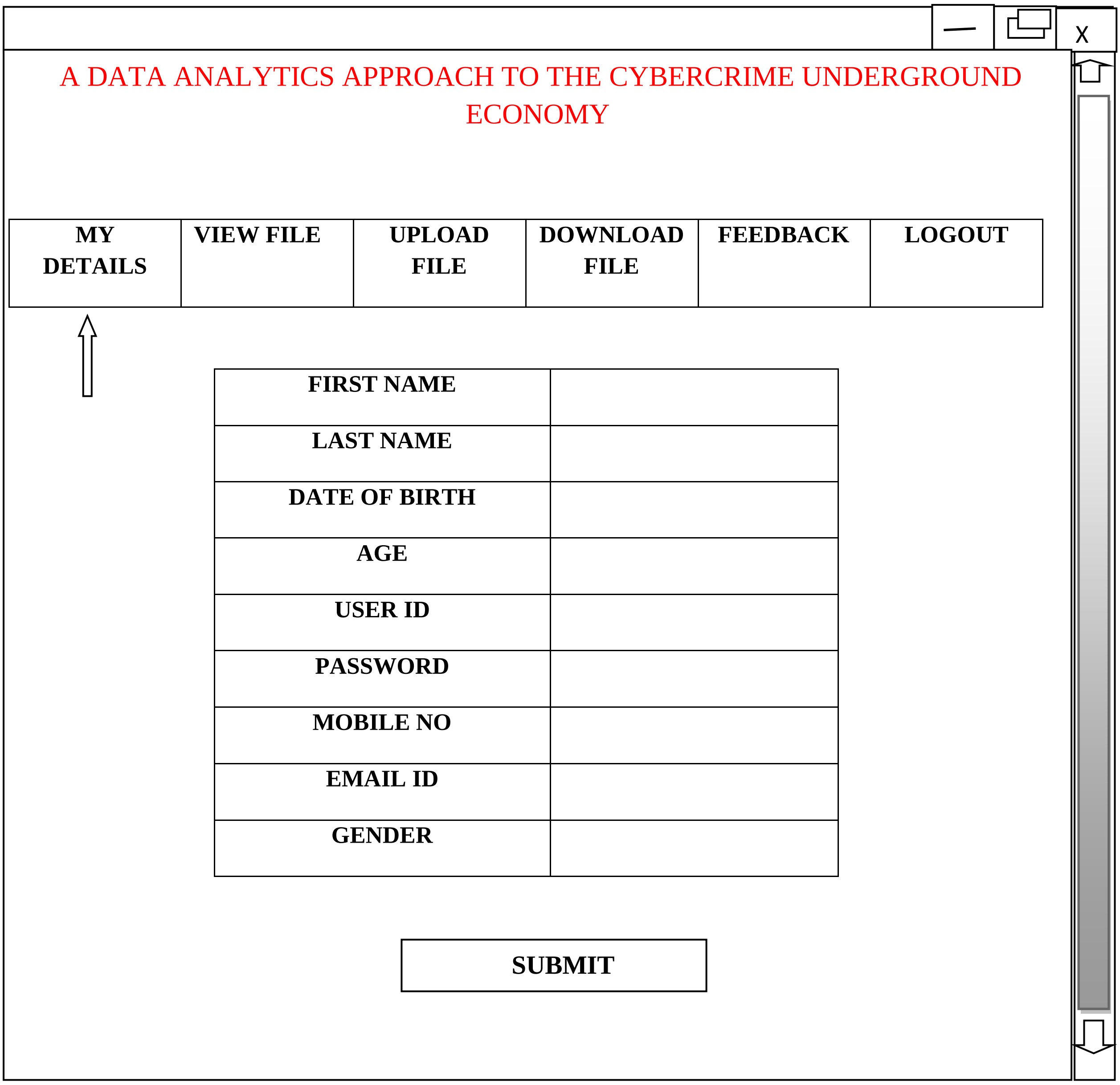
SCREEN LAYOUT

LOGIN PAGE :



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

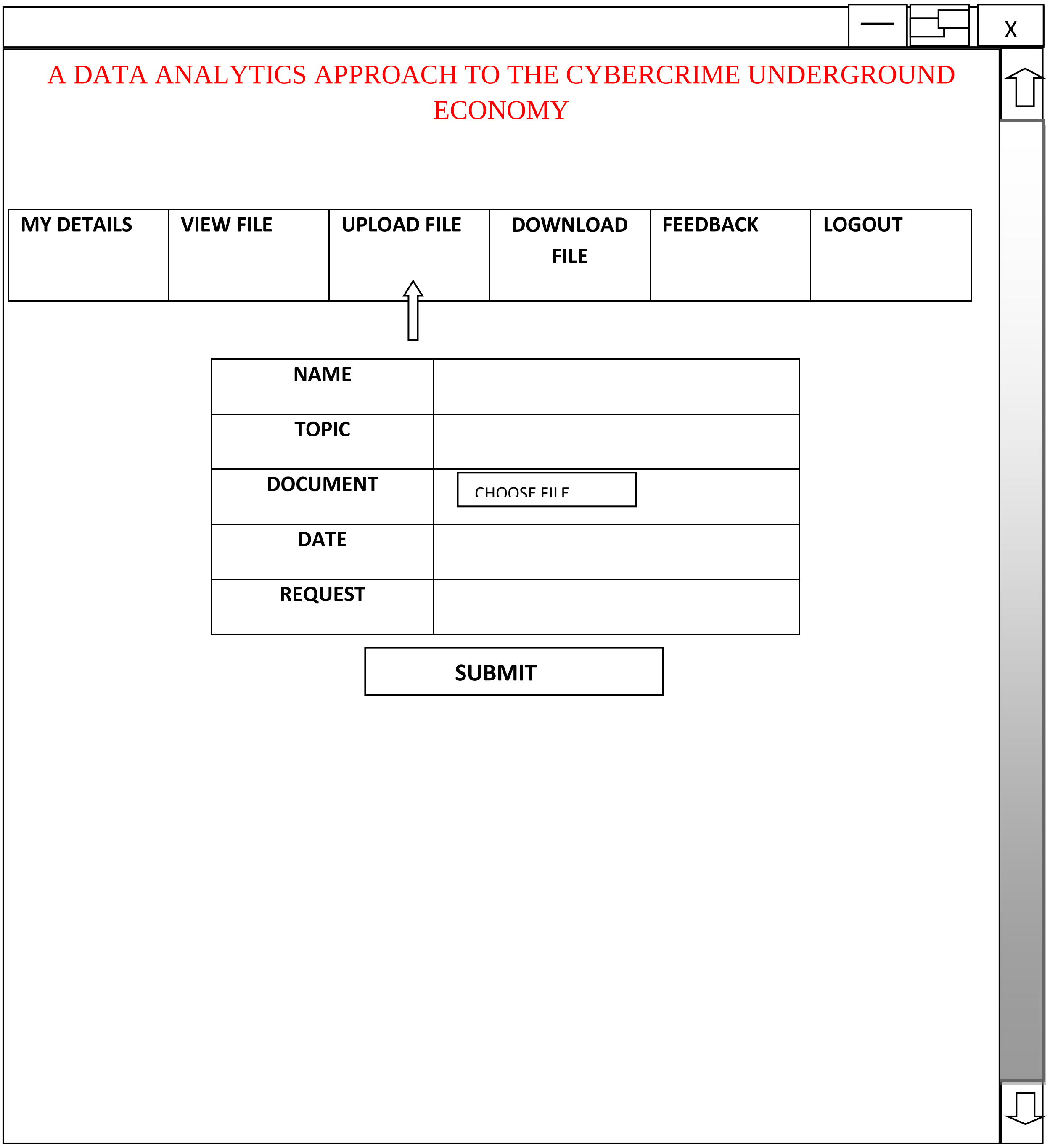
NEW USER REGISTRATION:



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

FIRST NAME	
LAST NAME	
DATE OF BIRTH	
AGE	
USER ID	
PASSWORD	
MOBILE NO	
EMAIL ID	
GENDER	

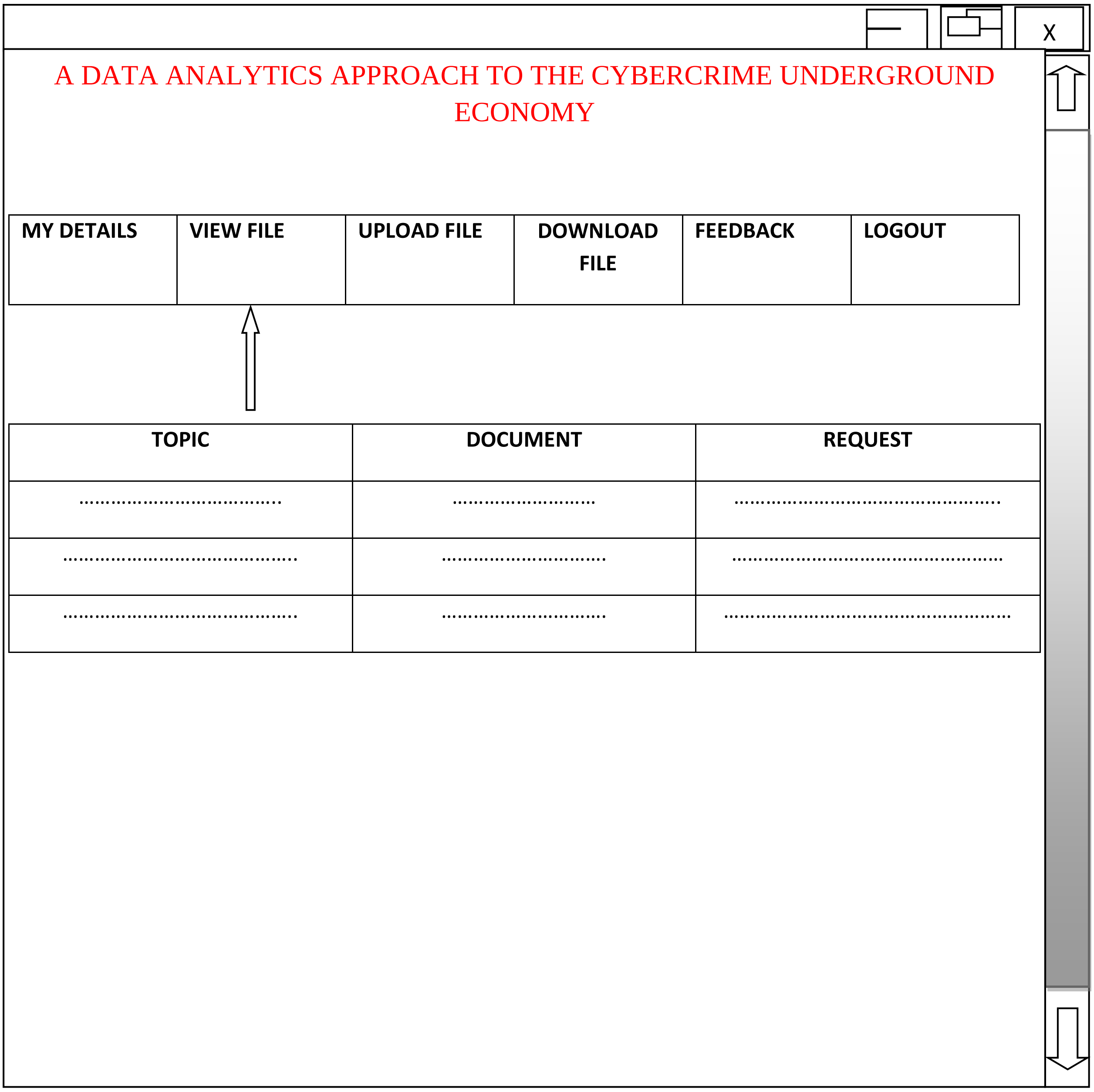
UPLOAD FILE PAGE:



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

NAME	
TOPIC	
DOCUMENT	CHOOSE FILE
DATE	
REQUEST	

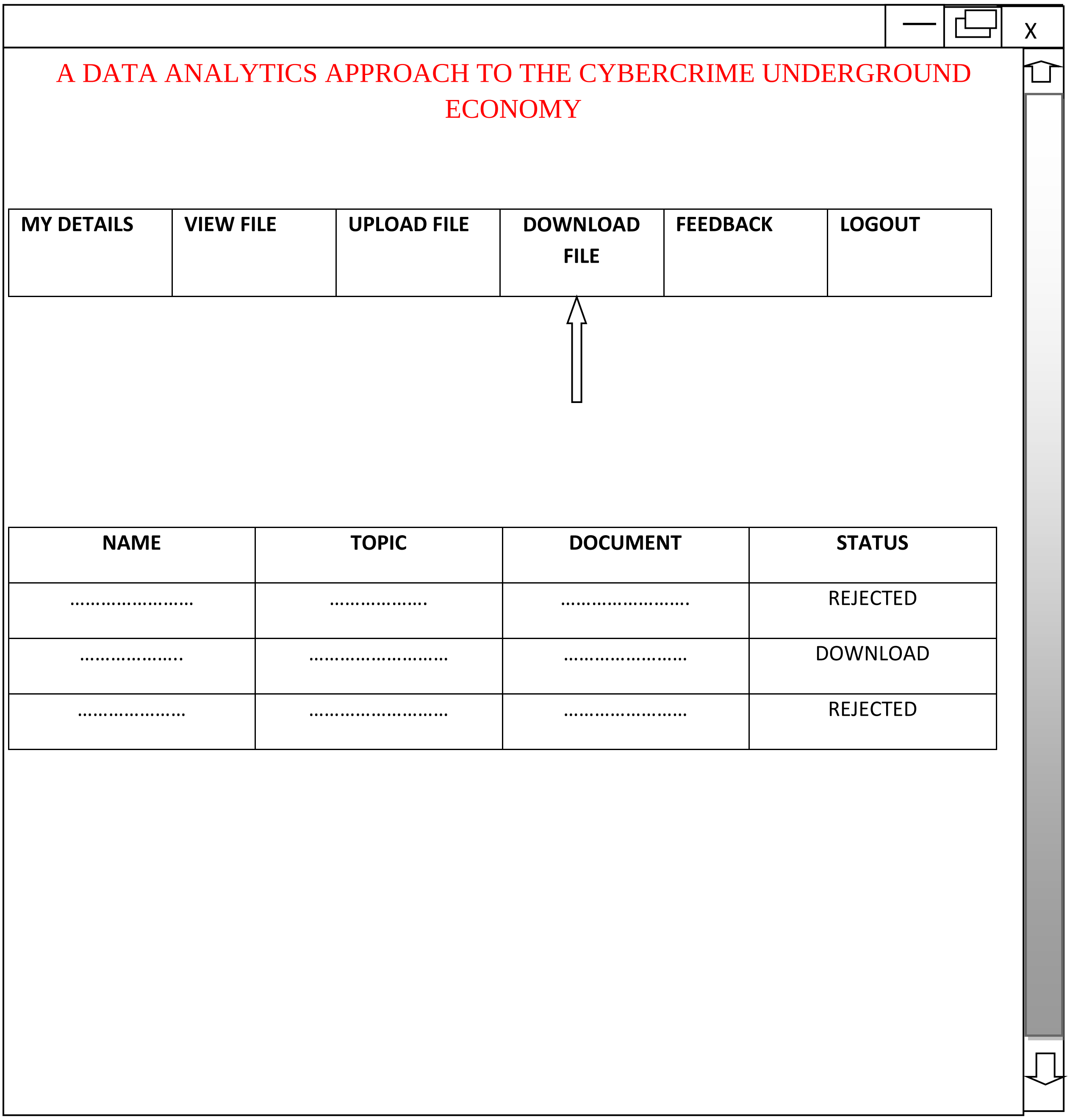
VIEW FILE PAGE:



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

TOPIC	DOCUMENT	REQUEST
………………………………..	……………………..	…………………………………………..
……………………………………..	…………………………..	…………………………………………….
……………………………………..	…………………………..	………………………………………………..

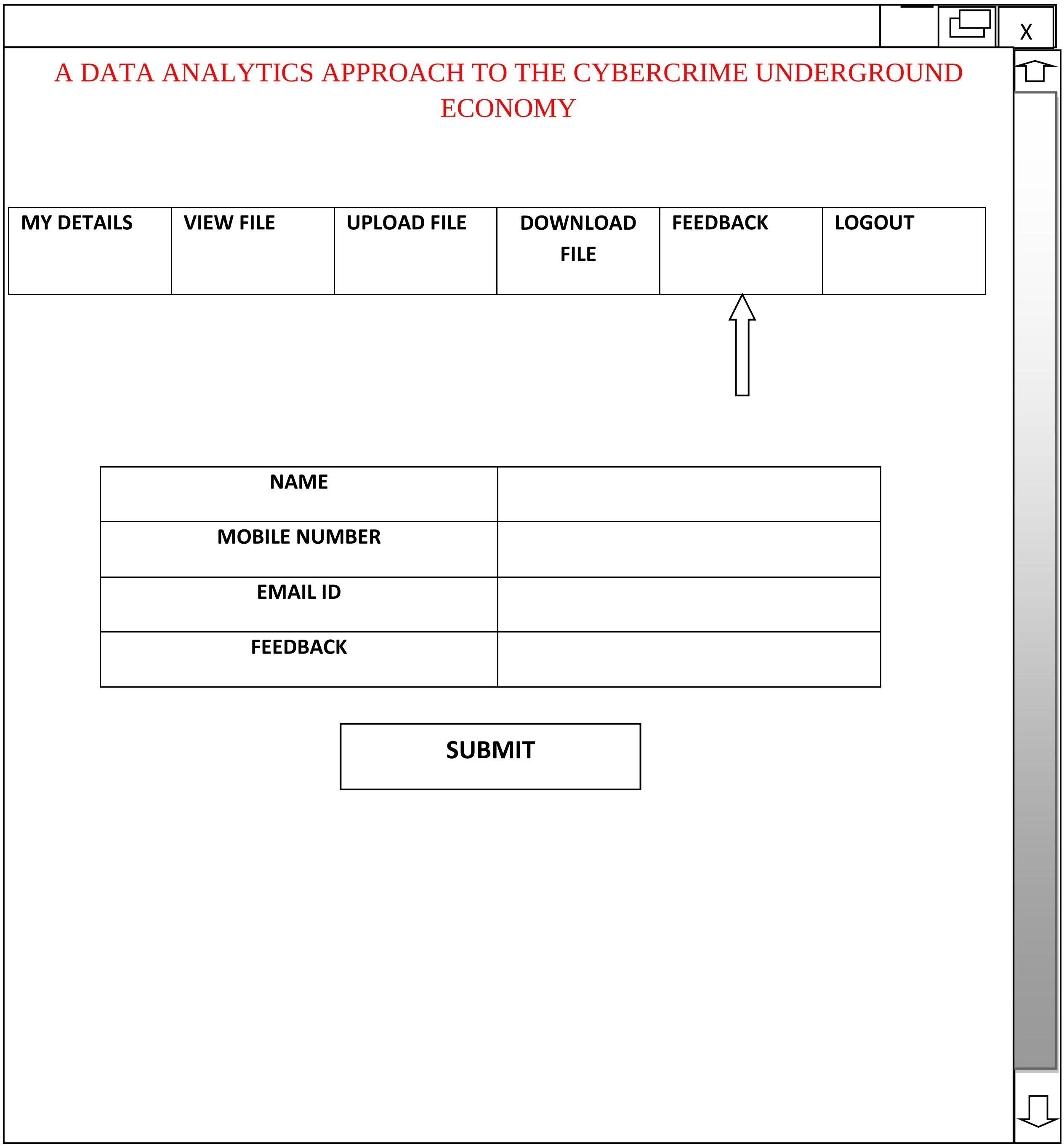
DOWNLOAD PAGE :



A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

NAME	TOPIC	DOCUMENT	STATUS
…………………….	……………….	……………………..	REJECTED
……………….	………………………	…………………….	DOWNLOAD
…………………	………………………	…………………….	REJECTED

FEEDBACK PAGE : This page describes about user feedback and details .


A DATA ANALYTICS APPROACH TO THE CYBERCRIME UNDERGROUND ECONOMY

NAME	
MOBILE NUMBER	
EMAIL ID	
FEEDBACK	

Chapter 8

DATABASE DESIGN

8.1 ER Diagram

An Entity-Relationship diagram (ERD) is a data modeling technique that graphically illustrates an information system’s entities and relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure. ER Diagrams are most often used to design or debug relational databases.

User:

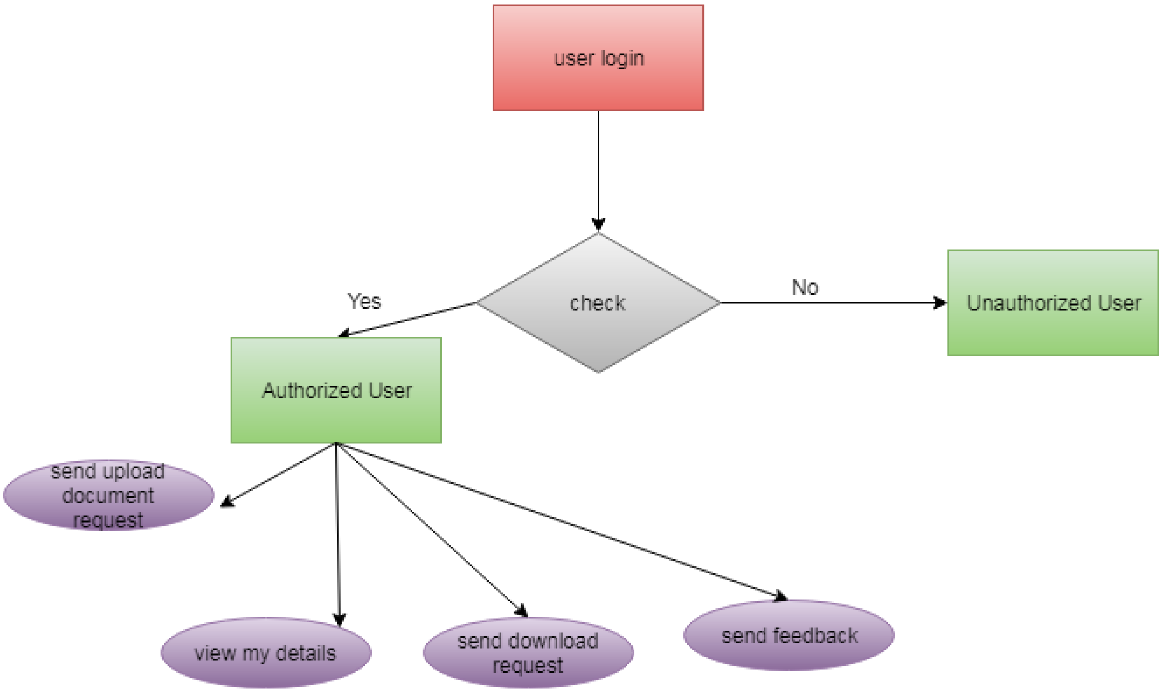


Figure8.1a:ER diagram for user module

Admin:

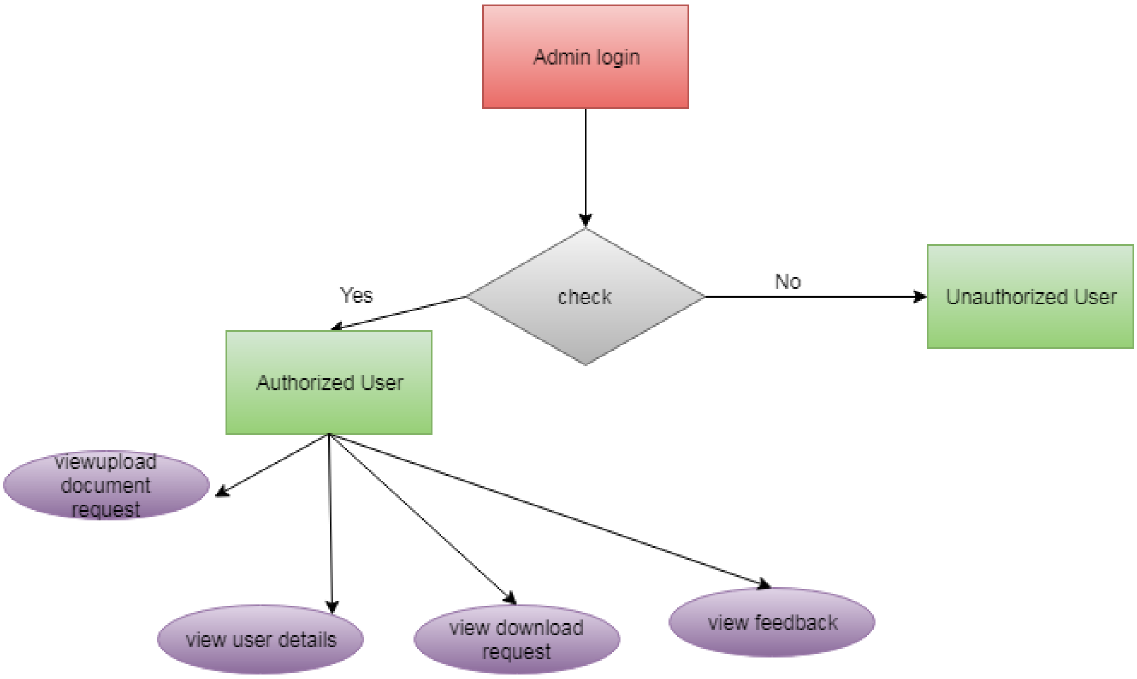


Figure8.1b:ER diagram for admin module

Flow Chart:

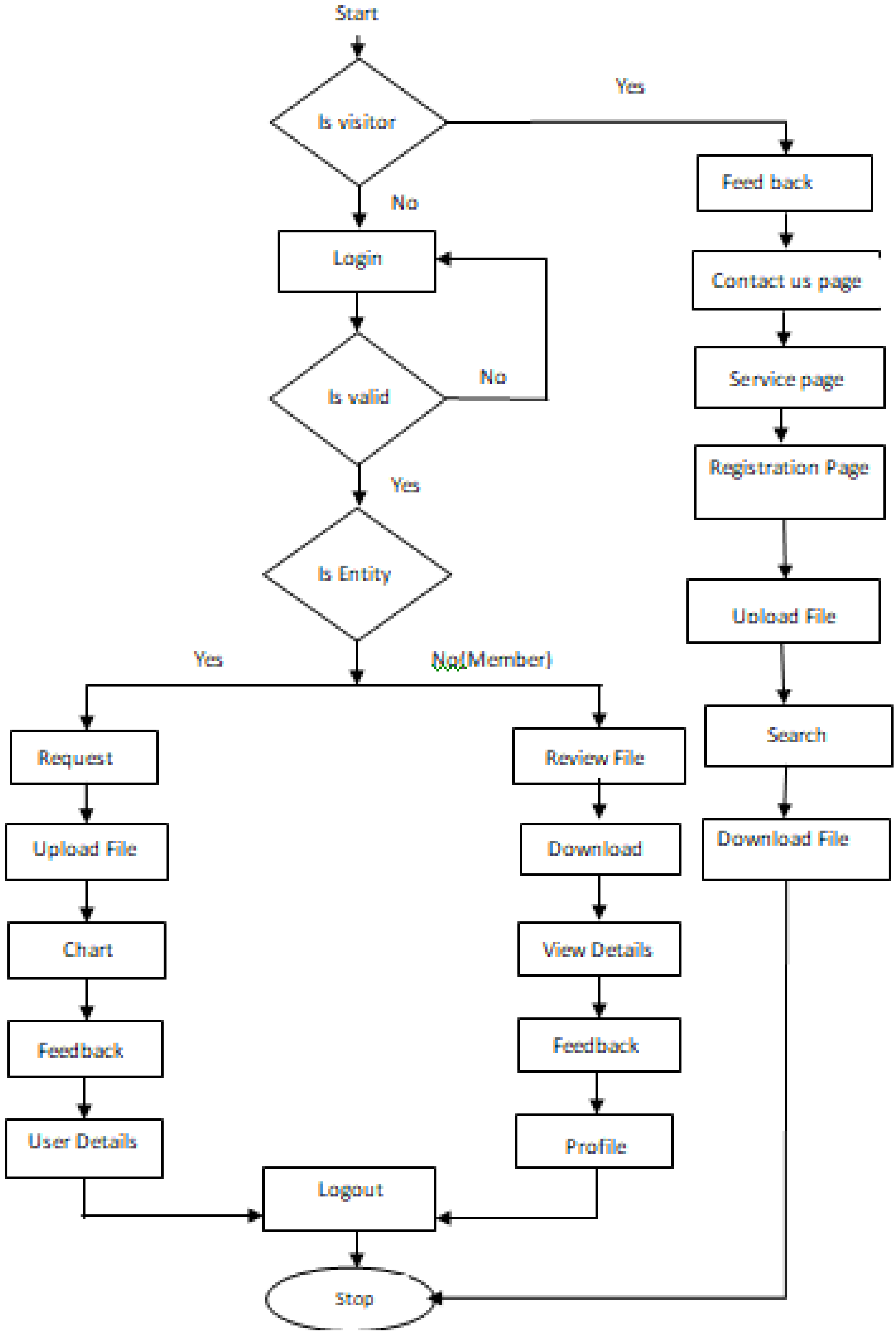


Figure8.1c:Flow chatr diagram for admin module

8.2 Data Flow Diagram

Data-flow diagram is a way of representing a flow of a data of a process or a system and information about the outputs and inputs of each entity and the process itself.

Business Entity/Admin :

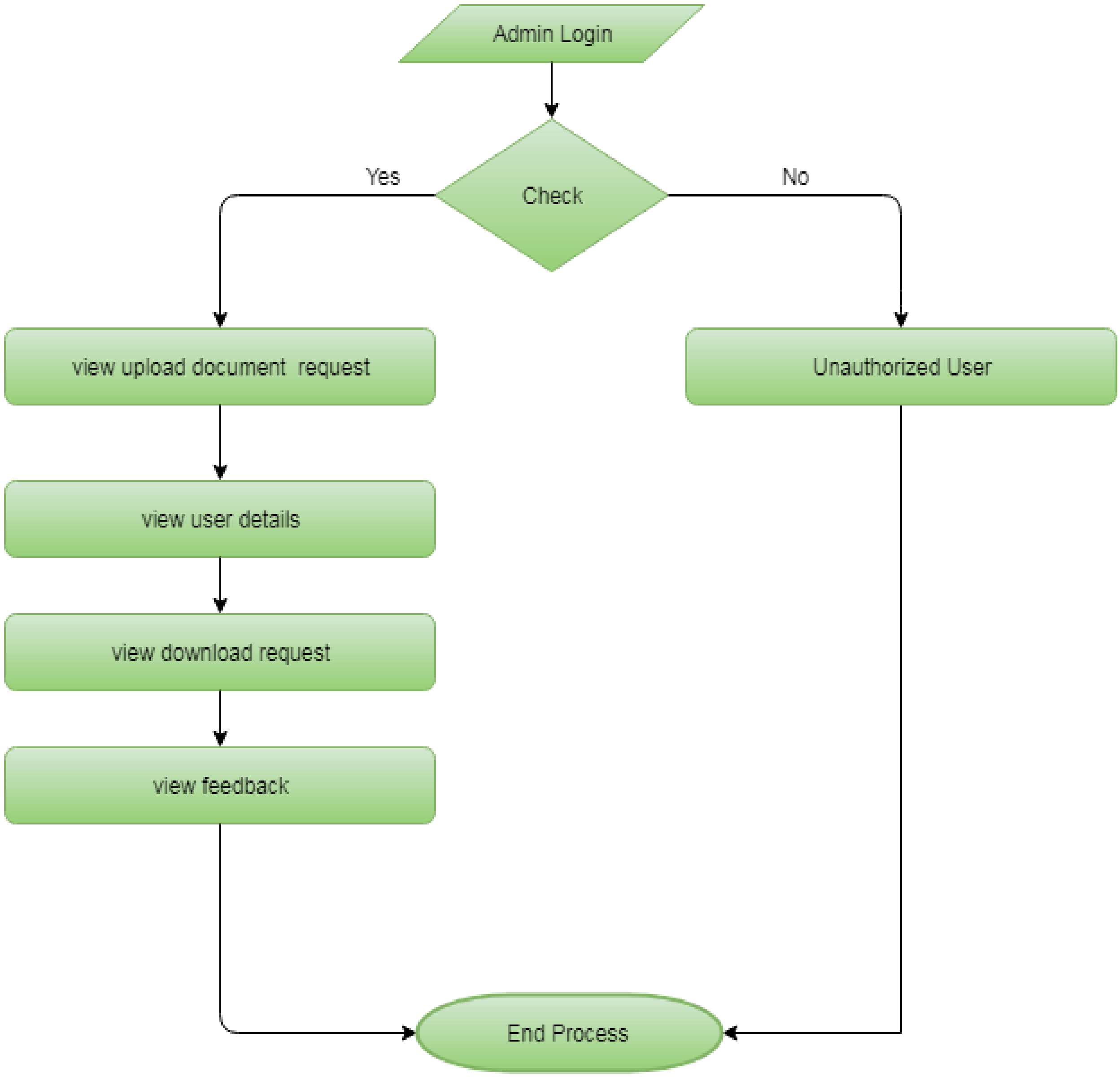


Figure8.2.a:Data Flow diagram for admin module

User:

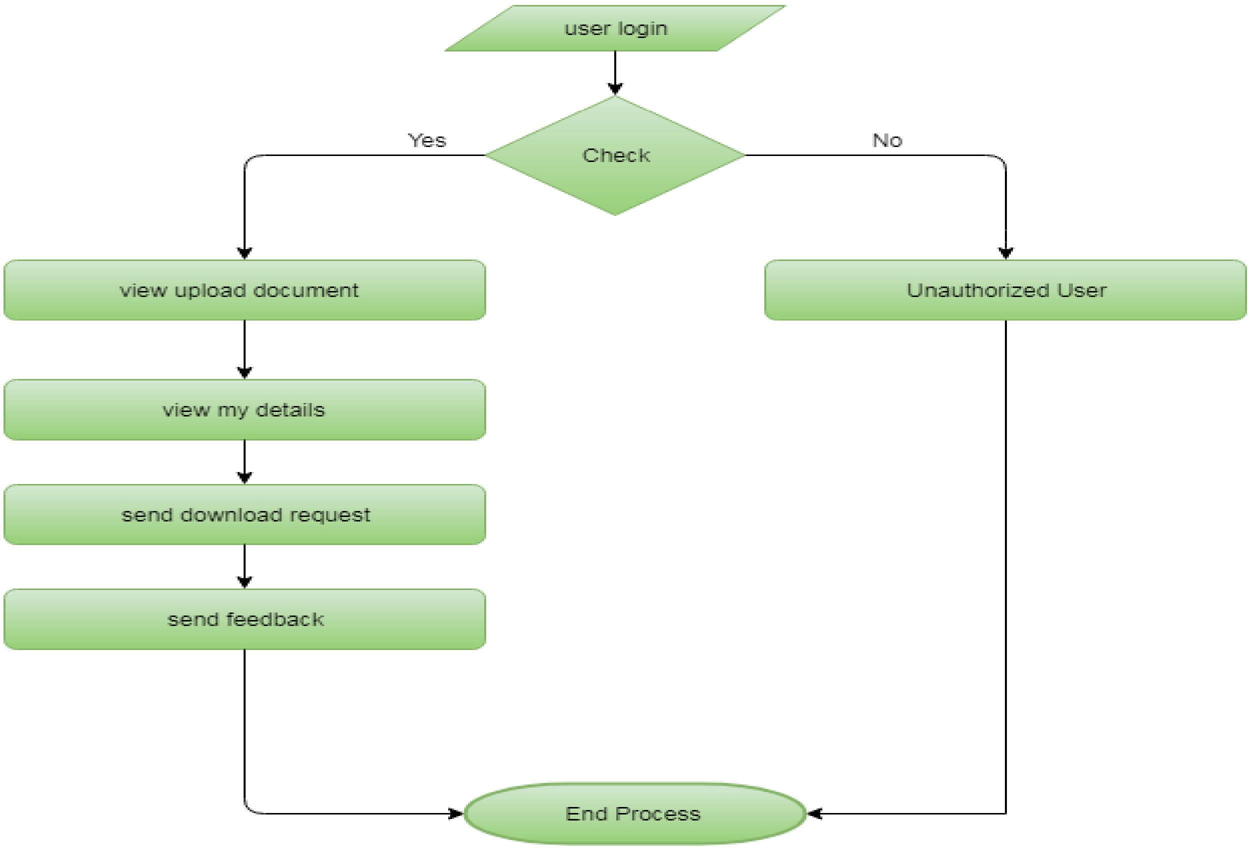


Figure8.2.b:Data Flow Diagram for user

8.3 Table Struture

Table Name: RegisterModel

Column	Type	Default
Id	int(11)	-
Firstname	varchar(100)	NULL
Lastname	varchar(100)	NULL
Dob	varchar(100)	NULL
Age	varchar(100)	NULL
Userid	varchar(100)	NULL
Password	int(11)	NULL
Mobilenumber	varchar(100)	NULL
Emailed	varchar(100)	NULL
Gender	varchar(100)	NULL

Table Name: UploadModel

Column	Type	Default
id	int(11)	-
Name	varchar(100)	NULL
Topic	varchar(100)	NULL
Document	varchar(100)	NULL
Date	varchar(100)	NULL

Request	varchar(100)	NULL
userDet_id	varchar(100)	NULL

Table Name: ChatModel

Column	Type	Default
Id	int(11)	-
senderId	int(11)	NULL
Chat	varchar(300)	NULL
userId_id	int(11)	NULL

Table Name: RequestModel

Column	Type	Default
Id	int(11)	-
accessone_id	int(11)	NULL
accesstwo_id	int(11)	NULL
Request	varchar(200)	NULL

Table Name: FeedbackModel

Column	Type	Default
Id	int(11)	-
Name	varchar(300)	NULL

Mobilenumber	varchar(300)	NULL
Emailed	varchar(300)	NULL
Feedback	varchar(300)	NULL

Table Name: UserChat

Column	Type	Default
Id	int(11)	-
Cusid	varchar(200)	NULL
Spkid	varchar(200)	NULL
Userchats	varchar(200)	NULL

Table Name: Algorithm_Model

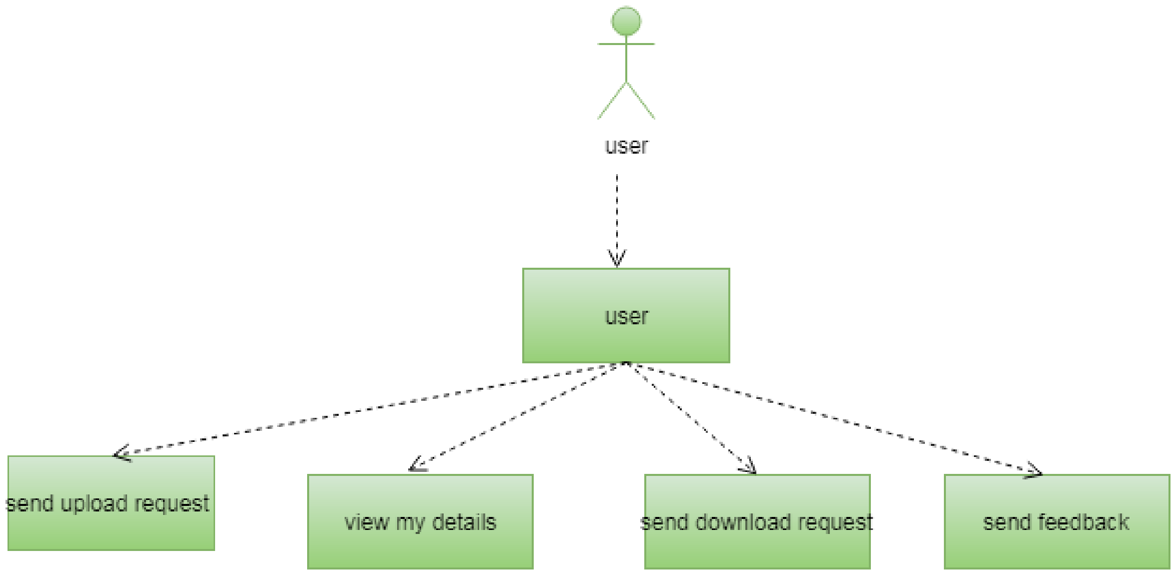
Column	Type	Default
Id	int(11)	-
algorithm_name	varchar(100)	NULL
Precisions	varchar(100)	NULL
Recall	varchar(100)	NULL
Accuracy	varchar(100)	NULL
True_Negative_Rate	varchar(100)	NULL

Chapter 9

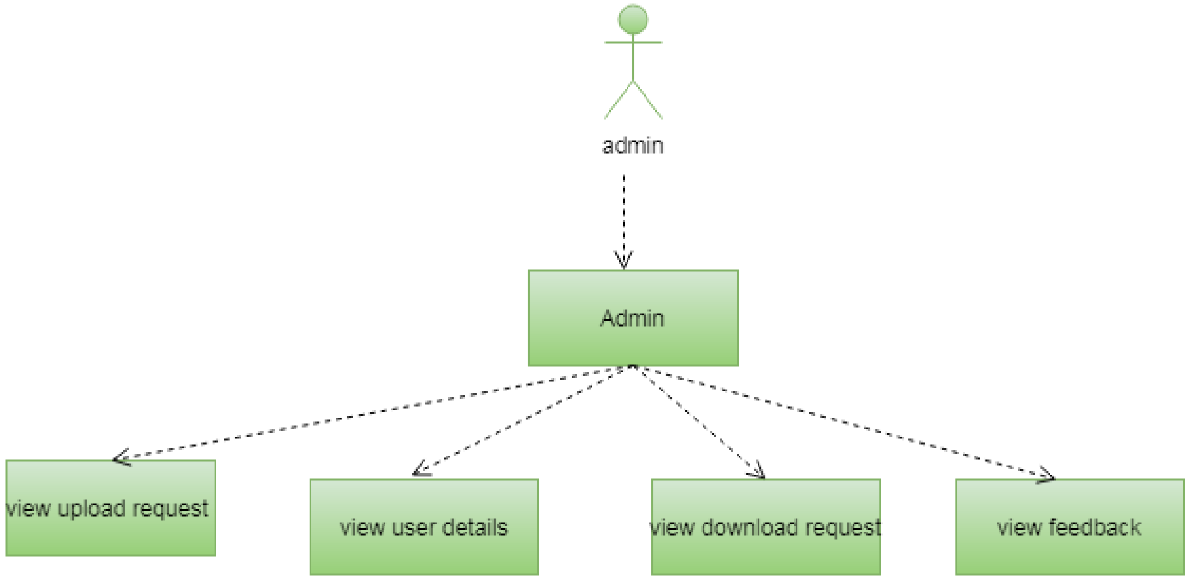
USE CASE DIAGRAM

A use case diagram at its simplest is a representation of a user's interaction with the system that shows the relationship between the user and the different use cases in which the user is involved.

Business Entity/User:



Admin:



9.1Sequence diagram

a) User

When Admin sign up successfully he/she can can view, add and delete eco products category and also he/she can view ,add and delete any eco products, as well as view and respond to customer orders and can also view customer feedback for future upgradation and at last admin also have an option to update his/her password.

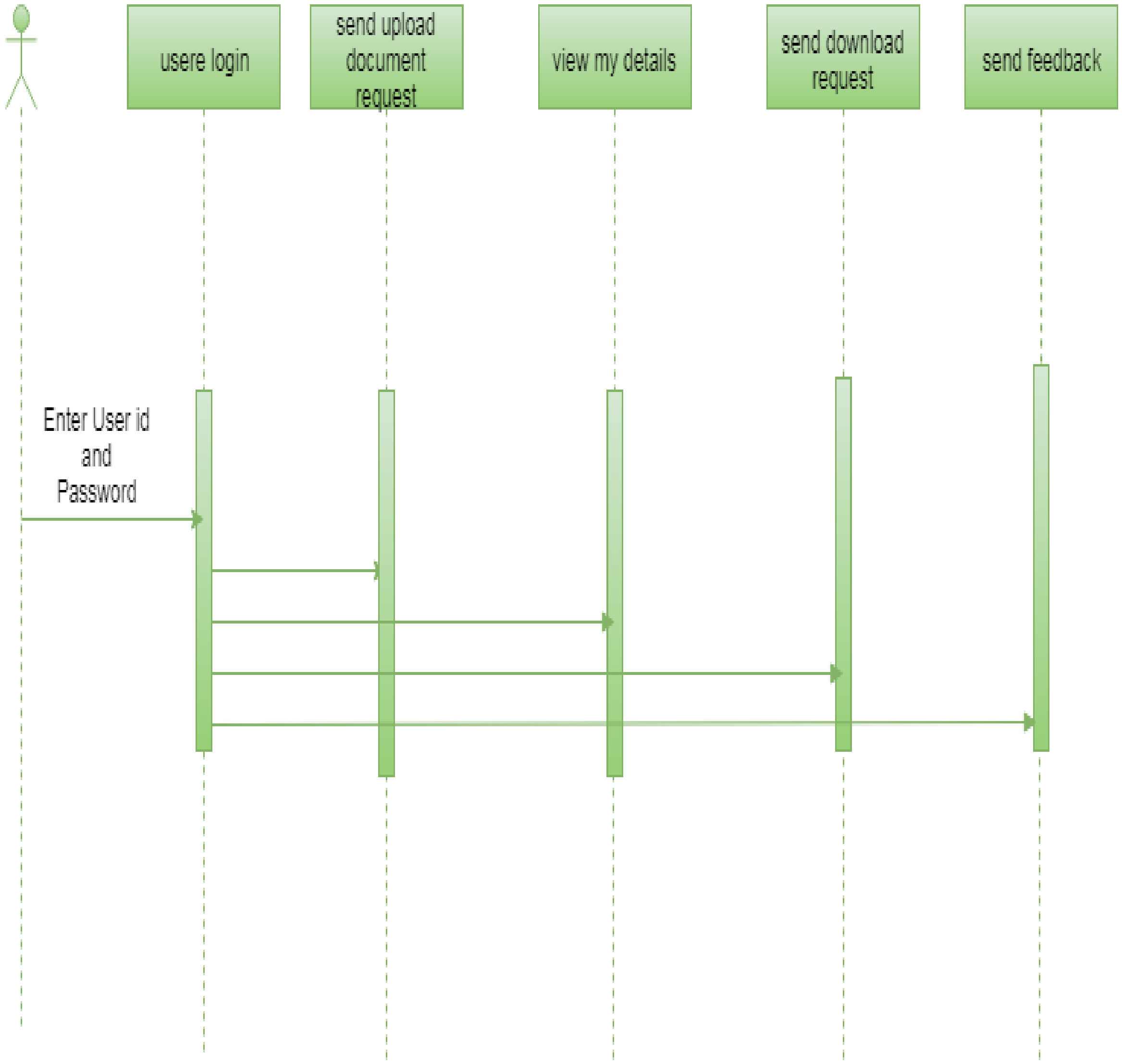


Figure9.1a: Sequence Diagram For User

(b)Admin:

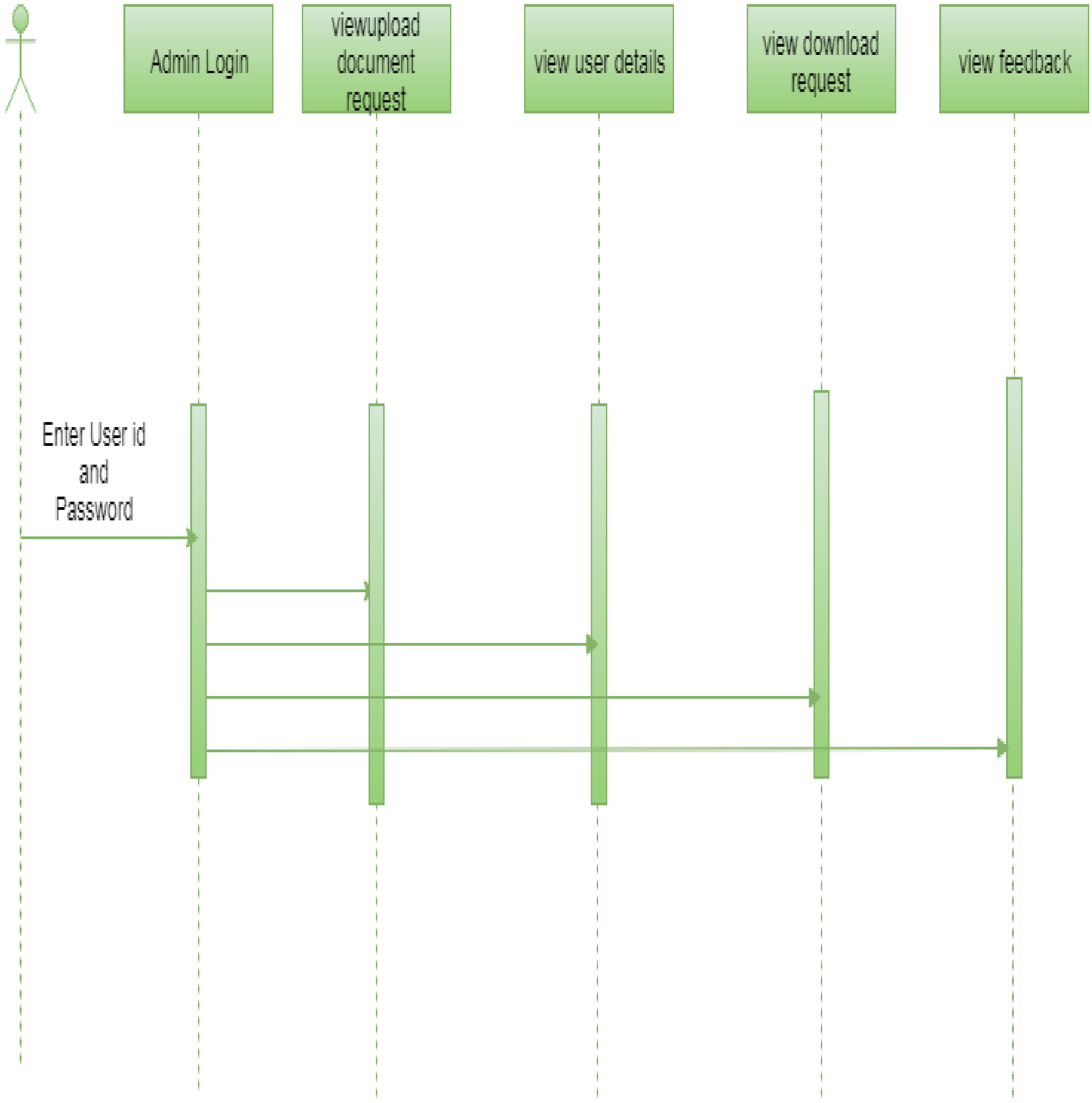


Figure9.1b: Sequence Diagram For Admin

When a user gets signed up, he/she can view or delete review order and can add to place a order , also can view order history and can add his/her feedback and at last he/she can also update his/her profile

9.2 Class Diagram

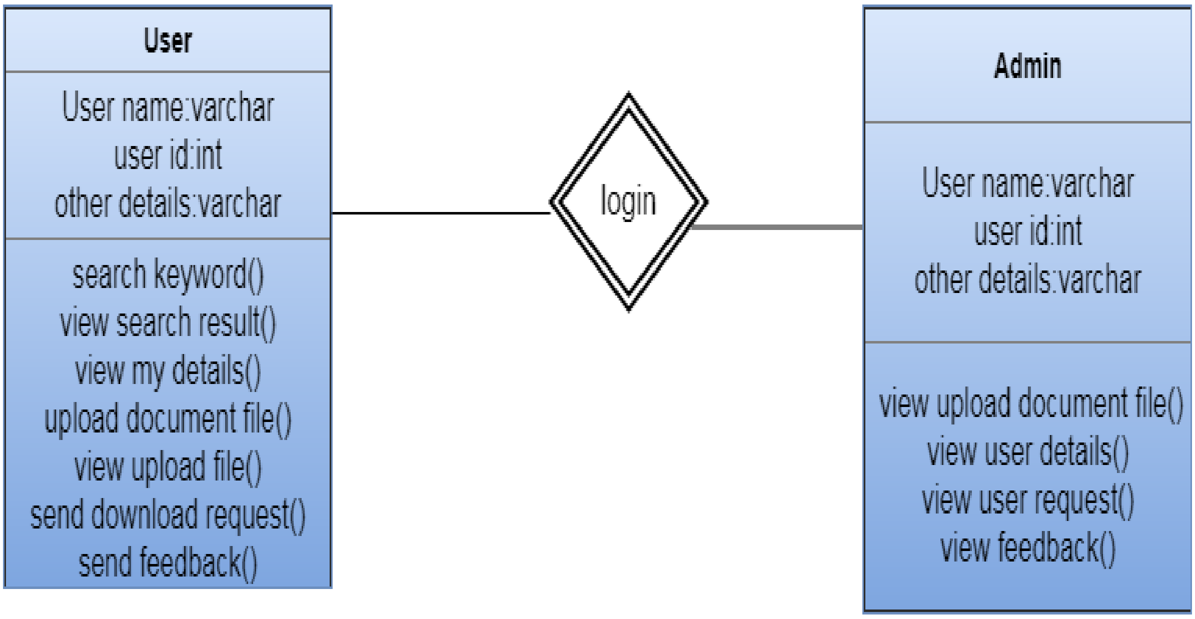


Figure9.2: Class Diagram

In software engineering, a **class diagram** in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects.

The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the structure of the application, and for detailed modeling translating the models into programming code. Class diagrams can also be used for data modeling.[1] The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed.

In the diagram, classes are represented with boxes that contain three compartments:

- The top compartment contains the name of the class. It is printed in bold and centered, and the first letter is capitalized.
- The middle compartment contains the attributes of the class. They are left-aligned and the first letter is lowercase.
- The bottom compartment contains the operations the class can execute. They are also left-aligned and the first letter is lowercase.

Chapter 10

SYSTEM TEST

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

TYPES OF TESTS

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures : interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

Unit Testing

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test case ID	**Description**	**Test steps**	**Expected value**	**Actual value**	**OK/Error**
1.	Verify login page	Input username and password	Login page	Invalid data	error
2	Verify login page	Input username and password	Login page	Login page	ok
3.	Verify registration page	Registration	User profile	Registration failed	error
4.	Verify registration page	Registration	User profile	User profile	ok
5.	Query is to be posted	Posting query	Query is posted	Unable to post the query	error
6.	Query is to be posted	Posting query	Query is posted	Successfully posted	ok
7.	Files to be upload	Upload file	File to upload	File name is entered	ok
8.	Files to be upload	Upload file	File to upload	Unknown file	error
9.	Files to be requested	Enter request file	File to be send	File name is Request	ok
12.	Files to be reuested	Enter request file	File to be send	File not found	error
13.	Chat Module	Enter text	Negative Text is entered	Possitive Text is entered	error
14.	Chat Module	Enter text	Possitive Text is entered	Possitive Text is entered	ok

Chapter 11

LIMITATIONS AND DRAWBACKS

Cybercrime has undergone a revolutionary change, going from being product-oriented to service-oriented .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.

- CaaS is referred to as a do-it-for-me service, unlike crimeware which is a do-it-yourself products.
- It is not secured process.
- Over under traction is invents.
- Download files, time is invited.
- The cyber-crime differs from general crime in many ways; we need to conduct a variety of analyses using a large data set.
- A previous study proposed a data mining framework for crime, dividing crimes harmful to the general public into eight categories:

  1.Traffic violations.
  2. Sex Crime.
  3. Theft.
  4. Fraud.
  5.Gang/Drug Offenses.
  6. Arson.
  7. Violent crime.
  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.
- Consequently, the CaaS business model can involve the following roles:

  i. writing a hacking program
  ii. performing an attack
  iii. commissioning an attack
  iv. providing an attack server (infrastructure) and
  v. 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.
- Periodic monitoring & analysis of the content of cybercrime marketplaces could help predict future cyber threats.

Chapter 12

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.

CONCLUSION

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 (preventive measures, related to CaaS) 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.

REFERENCES

[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.