
# A URL-based Phishing Attack Detection and Data Protection Model

**M.Sc. THESIS**

**Yonathan Bukure Racho (**PGCSW/018/10**)**

**HAWASSA UNIVERSITY, HAWASSA, ETHIOPIA**

**May, 2021**

# A URL-based Phishing Attack Detection and Data Protection Model

**Yonathan Bukure Racho (**PGCSW/018/10**)**

**ADVISOR: BASANT TIWARI (Ph.D.)**

**Co-ADVISOR: DANIAL TESFAY (M.Sc.)**

**A THESIS SUBMITTED TO THE**
**DEPARTMENT OF COMPUTER SCIENCE,**
**HAWASSA INSTITUTE OF TECHNOLOGY,**
**FACULTY OF INFORMATICS**
**HAWASSA UNIVERSITY**
**HAWASSA, ETHIOPIA**

**IN PARTIAL FULFILLMENT OF THE**

**REQUIREMENTS FOR THE**

**DEGREE OF**

**MASTERS OF SCIENCE IN COMPUTER SCIENCE**

**HAWASSA, ETHIOPIA**

**May, 2021**

## DECLARATION

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

Name: **Yonathan Bukure Racho (**PGCSW/018/10**)**

Signature: _____

I, hereby certify that, this thesis has been submitted for examination with my approval as thesis advisor and co-advisor.

Name: Basant Tiwari (PhD)

Signature: _____

Place and Date of Submission: _____

Name: Danial Tesfaye (M.Sc.)

Signature: _____

Place and Date of Submission: _____

**APPROVAL SHEET**

As members of the Examining Board of the Final MSc. Open Defense, we certify that we have read and evaluated the thesis prepared by **Yonathan Bukure Racho (PGCSW/018/10)** entitled "**A URL-based Phishing Attack Detection and Data Protection Model**", and recommend, that it be accepted as fulfilling the thesis requirement for the degree of Masters of Science Degree in Computer Science.

| | | |
|---|---|---|
| --- | --- | --- |
| Name of Chairman | Signature | Date |
| --- | --- | --- |
| Name of Advisor | Signature | Date |
| --- | --- | --- |
| Name of Co-Advisor | Signature | Date |
| --- | --- | --- |
| Name of Internal Examiner | Signature | Date |
| Sileshi Demesie (PhD |  | 24/08/2021 |
| Name of External Examiner | Signature | Date |

Final approval and acceptance of the thesis is contingent upon the submission of the final copy of the thesis to the SGS through the Department of Graduate Council (DGC) of the candidate's major department.

Thesis approved by

| | | |
|---|---|---|
| --- | --- | --- |
| DGC/SGC | Signature | Date |

## DEDICATION

**Dedicated to My Family**

## ACKNOWLEDGMENTS

Firstly, I would like to thank God, whose grace has let me to this important time of my life. I am thankful and appreciative of my supervisor, Dr. Basant Tiwari for his valuable contributions and continuing efforts to the success of this thesis. He has imparted to me knowledge that is both practical and invaluable to my future endeavors especially insight to the social engineering attack. He has also gone beyond his duties of a supervisor to act as a mentor and friend. I would also like to thank my co-supervisor, Mr. Danial Tesfaye. He has given me valuable advice and upgrade my technical knowledge and skills. Without his advice and suggestions, this thesis would not have been possible. Also, I acknowledge all my teachers and staff of Department of Computer Science, IoT, Hawassa University, which have been encouraged and supported during my studies.

Last but not least, I would like to give special thanks to my family, friends and anyone who is not mentioned here but had helped me in one way or another.

## ABSTRACT

Internet users are increasing rapidly in an uninterrupted way that is influencing the way of living. Every day billions of websites are accessed over the globe to facilitate different usage to people. This positive reinforcement is also resulting in internet abusing by hackers for their benefits. Most of the time internet abusing has experimented with over mobile phones or emails. The users are victimized by those abuse even without knowing that they are misused by hackers. Social engineering has become the tool for the hacker to manipulate users psychologically to reveal secret information.

Phishing is a kind of social engineering attack with the potential to do harm to the individual or overall organization. Cybercriminal called Phisher comes up constantly in contact with individuals with creative ways to compromise the secret assets. Phishers uses the malicious URLs that are embedded over the webpage with severe threat and appears legitimate. When user clicks these links, redirects to malicious webpage where attackers ask some secrete information by misguiding user. Such kinds of attacks must be properly addressed.

This thesis is focused on URL based phishing detection and data protection against such kind of attacks. Thus, the contribution of this thesis is divided into two phases that are: (1) URL based phishing attack detection, and (2) Protection of individual/organization assets. For the first phase, this thesis explored and implemented four machine learning algorithms like Decision tree, Random Forest, Naive Bayes, and Logistic Regression. Further performances of these algorithms are evaluated and compared against training and testing dataset. Based on performance result obtained, the best algorithm is recommended. For the second phase, thesis proposed a data protection model using a hybrid encryption method that combined AES and RSA algorithms. This model ensures the confidentiality of information assets as well as protect them against various kind of attacks. Overall proposed work is implemented in the Python programming language.

The phishing detection phase concluded that Random forest outperforms and gave the highest accuracy of detection after important feature selection as compared to other algorithms. Results analysis conclude 96.89% and 99.06% detection accuracy over testing and training dataset respectively in Random forest. Similarly, the data protection phase encrypted and decrypted the data files very fast i.e., within few milliseconds and ensured the confidentiality of data in transit

as well as in storage. The proposed hybrid algorithm uses the key sizes of 128 and 1024 bits for RSA and AES, respectively. We run the algorithm over different files of different size and type. For example, this encryption algorithm took 184 ms and 149 ms for encryption and decryption of 1.7 MB clinical management data file, respectively.

Finally, the thesis is concluded with proposed contributions and future recommendations.

**Keywords**: Social engineering; Phishing attack; Attack detection; Machine learning algorithm, Data protection; Encryption; Decryption

# TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF ACRONYMS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ANN | Neural Networks |
| APWG | Anti-Phishing Working Group |
| AR | Association Rule |
| CCTV | Closed Circuit Television |
| CIA | Confidentiality Integrity Availability |
| CP-ABE | Cipher Text Policy Attribute-Based Encryption |
| CSV | Comma Separated Values |
| CVV | Card Verification Value |
| DES | Data Encryption Standard |
| DNS | Domain Name System |
| DSRM | Design Science Research Methodology |
| DT | Decision Tree |
| ELM | Extreme Learning Machine |
| GBT | Gradient Boosting Tree |
| GCD | Greatest Common Divisor |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| ICT | Information Communication Technology |
| ID3 | Iterative Dichotomies 3 |
| IDS | Intrusion Detection System |
| IP | Internet Protocol |
| IPS | Intrusion Prevention System |
| ISP | Internet Server Providers |
| KNN | K-Nearest Neighbor |
| LR | Logistic Regression |
| MAC | Media Access Control |
| MD 5 | Message Digest 5 |
| MiTM | Man-In-The-Middle |
| ML | Machine Learning |

| | |
|---|---|
| NB | Naïve Bayes |
| PBC | Pairing-Based Cryptography |
| PCA | Principal Component Analysis |
| RC-2 | RON's Code 2 |
| RF | Random Forest |
| RFE | Recursive Feature Elimination |
| RSA | Rivest Shamir Adleman |
| SE | Social Engineering |
| SEADMv2 | Social engineering attack detection model Version 2 |
| SEPTT | Social Engineering Prevention Training Tool |
| SET | Social Engineering Toolkit |
| SFH | Server Form Handler |
| SHA | Secure Hash Algorithm |
| SMS | Short Messaging service |
| SVM | Support Vector Machines |
| UCI | University of California Irvine |
| URL | Universal Resource Locator |
| USB | Universal Serial Bus |
| WWW | World Wide Web |

# CHAPTER ONE

# INTRODUCTION

## 1.1.Background

The growth of the internet is getting higher and higher day by day, but with this higher usage, new techniques to attack organization's websites are also growing. Hackers are using various tactics to deceive a general user. Being an internet user, they can test you by providing an inappropriate picture, webpage and redirect you to inappropriate pages which are malicious and made up of source code like JavaScript[1]. One of the categories of hackers are phishers, who work by trading off a genuine space to make phishing sites or by bargaining a current site to incorporate malicious contents to divert a user to a malignant server where client information can be downloaded. They can play with clients by providing fake space names, for example, pay5al.com, pay-pal.com, or PayPal.sign-in.online, which resemble favourable site PayPal.com[2] and results in cheating with the user. The following subsection describes it more in detail.

## 1.2.Social engineering attacks

Social engineering attacks are rapidly increasing in today's internet era and are weakening the cybersecurity chain. They aim at manipulating individuals and enterprises to reveal valuable and sensitive data in the interest of cyber criminals [3]. Although with the usage of recent security deployments like firewalls, cryptographic techniques, IDS/IPS systems and anti-virus software systems, social engineering attacks are becoming challenges that breaching the security of user and enterprises credentials. As far as human mentality, behavior and relationships are concerned, they trust other humans rather than machines and technologies even it is artificial intelligence enabled. Thus, humans become the weakest link in the security chain. This results in divulging confidential information by innocent internet user through malicious human interactions who psychologically influence a person to break the security procedure[4]. Due to such kind of human interactions, social engineering attacks become the most powerful attacks because they threaten all systems and networks. These attacks cannot be prevented using available security solutions, including hardware or software security solutions as long as people are not trained to prevent these attacks.

Although social engineering attacks come across in various varieties they have a common pattern with similar phases. This common pattern involves four phases: (1) collect information about the target; (2) develop a relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces [5] . Figure 1.1 illustrates the different stages of a social engineering attack.

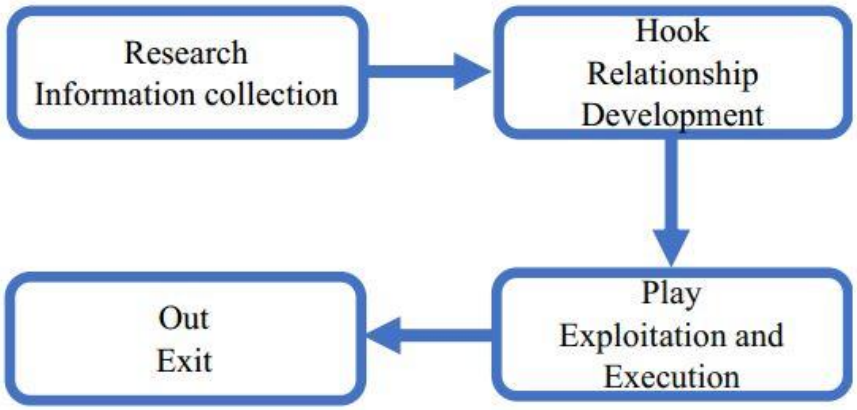



Figure 1.1. Social engineering attack stage [6]

The **research phase** is also called the information gathering phase in which hacker selects a victim based on some requirement. Subsequently, in the **hook phase**, hackers start trust building with victim through direct calling or communication through email. Once trust is made up, the hacker influences the victim emotionally to provide sensitive information or perform security mistakes, that is he play, exploit and execute the attack called **the play phase**. Lastly, after ditching the victim, the attacker quits without leaving any proof, that is called **out phase** [7].

Phishing is a kind of social engineering attack in which attacker that is known as “Phisher”, try to thieve user credential and information by mimicking an entity on which victim user’s trust. Phisher mostly targets user’s secret credentials including usernames, passwords, credit card numbers, social security numbers, and so on. Nowadays, E-mail is most common way to generate phishing attack, in which attacker sends malicious mail to user, clamming to be a trusted user mostly from banking or financial institution to acquire the account number, password or credit card credential like card password or CVV number. The email’s message attempts to convince the user to perform some actions which typically begin with clicking an embedded URL that is included in the body of the email. Such attempts leads the victim to a

website controlled by the phisher that claims to belong to the trusted entity. The website is often created to mimic the targeted entity's website in order to further deceive the user. Any information that the user provides to the website is captured and later exploited by the phisher [8] .

A typical phishing attack, as described in Figure 1.2, starts by designing a fake website and then sending a fake email to an Internet user which tries to convince him to follow a fraudulent link to a fake website which looks exactly like a legitimate one. If the user follows the spoof link, the attacker starts to collect user's security information which will later be used for unlawful activity.

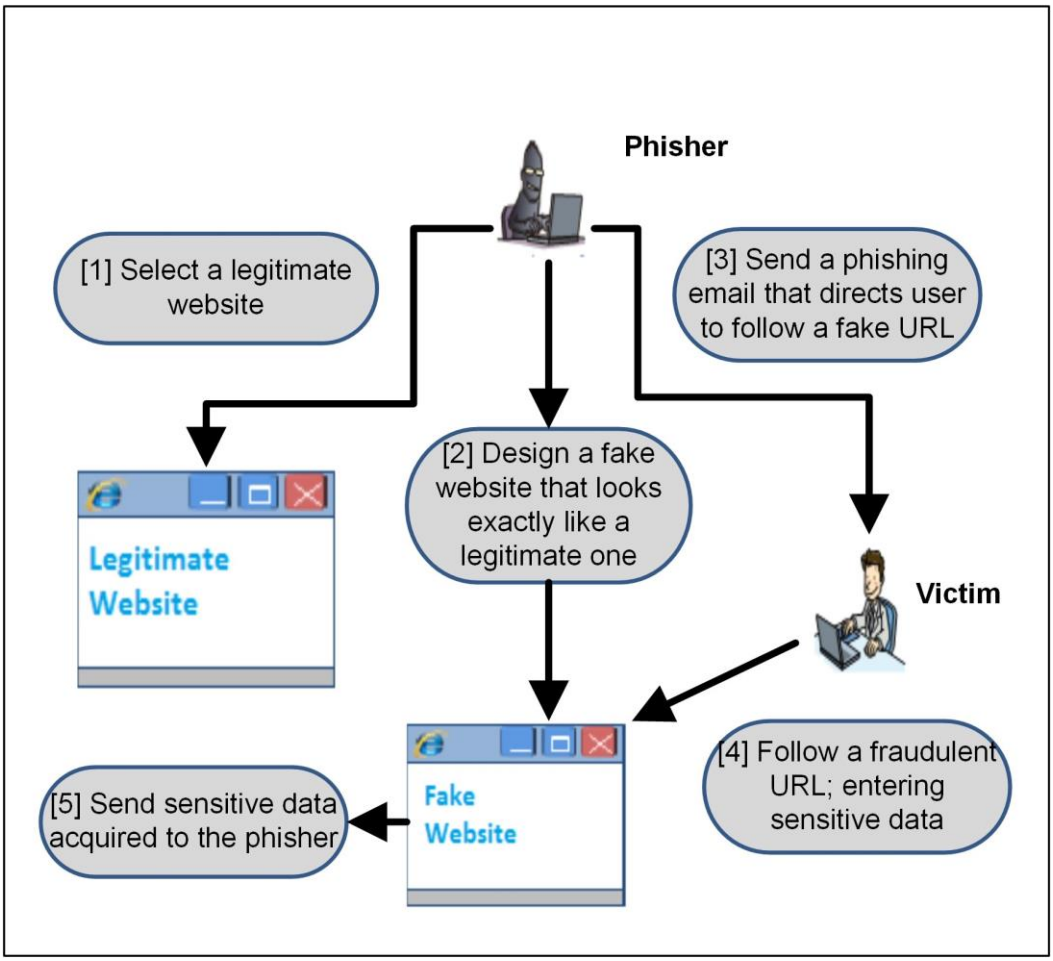



Figure 1.2: Typical phishing attack[8]

As far as cyberattacks are concerned, phishing is one of the ever-popular techniques hackers use for malicious intentions. Phishing combines technical tricking and social engineering activities in an attempt to gain personal and sensitive information such as logion id and password, credit card

user id and password or CVV or business secrets from the victim. This all happened by sending a spoofed mail or short messages (SMS) masquerade as a legitimate request received by a well-known entity. These mails incorporated malicious links that readdresses potential users to a forged website that is intended to resemble the authorized website of the fake entity. These sites now encourage the users to fill the private user's information/credentials that are further be misused by phishers/hackers. Phishers uses adaptive strategies to attack that become the major problem in detection of such attack. Hackers bypasses most defense technique easily to generate the phishing websites. Phishers continuously updates their toolkits to generate phishing websites that can escape all kinds of available defense mechanism. Following figure 1.3 shows the development of phishing attack between 2005 and 2016 in the living society that is reported by Anti-Phishing Working Group (APWG) [9]. This motivates to develop robust detection technique that can establish proper resiliency toward adaptive techniques used by the hackers/phishers.

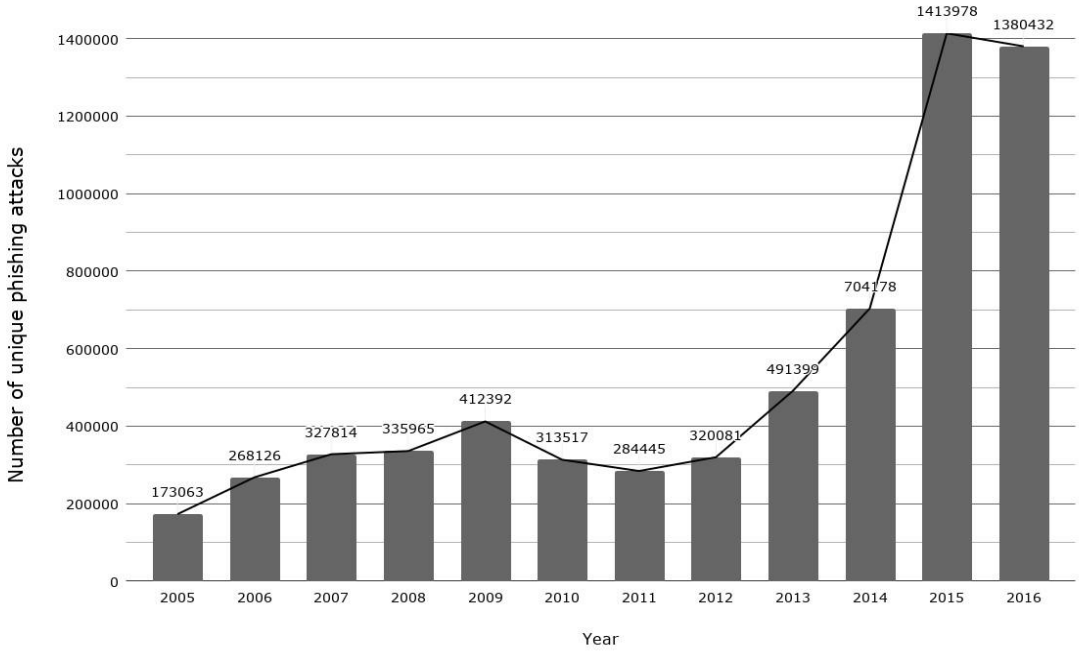



Figure 1.3: Number of unique attacks reported by APWG [9]

Machine learning (ML) is nowadays become latest technique and trend to detect such kind of phishing attacks which give rapid and accurate decision in detection of phishing mails and attacks.

This thesis proposed an approach to phishing detection using various machine learning algorithms, which utilizes features extracted from the URL. Further thesis focused on information security that provide a practical advantage to protect the information assets of organization. Thus, thesis focused on network monitoring and security that has the ability to monitor and protect the network as a whole i.e., detection and prevention against URL type phishing attack. This means that a URL-based phishing detection and protection provide better protection to all users in the network.

This thesis evaluated various machine learning approaches like Decision tree, Random forest, Naïve Bayes and Logistic Regression for performance evaluation over social engineering dataset of 11055 tuples with 30 features related with URL based phishing attack. Here, it is claimed that proposed model with Random forest perform well with better accuracy. Further thesis employed hybrid cryptographic technique to protect the sensitive data from the attacks. The goal of data protection is to ensure that only authorized users can view, and use informational assets. This would secure the data from attacker when him/her access the data even after getting personal secrets from victim. For ensuring this, researcher security layer in the proposed model that used the encryption/decryption process to provide information security that ensure that original data would be access by authorized entity. This security controls add another layer of protection in the system to protect the assets. To achieve this goal, security system implements data protection model using hybrid cryptographic technique that combined AES and RSA algorithm.

### 1.3.Problem Statement

Nowadays, information security, privacy and social engineering attack is very important concern for protecting personal, commercial or even state credential and secrets. Modern community is dependent on the Internet to perform important tasks since most of the services becomes online. This increased the excessive use of the Internet through which thing completed online as well as users communicate to each other and shares information to complete the task. This way to complete the task gave rise to the vulnerability to be misused by the illegitimate user. Such user introduces themselves as an authorized entity in the commutation and gain personal or corporate informational assets. These users have some kind of intelligence including technical as well as psychological that helped them to gain some personal data through tempering the ICT assets as

well as tempering the mind of user or behavioral study that result in ultimately the loss of user or organization.

Nowadays commonly social engineering attacks are affecting to individuals by making themselves even more vulnerable by not expecting ever to be a victim of such an attack. Many individuals never even know that they have actually been a victim. Hacker mask themselves as a reliable organization's employee and send the Emails and SMS links that redirect the victim to masqueraded websites. Most people are not aware of such attacks and unknowingly they have been cheated and personal information has been misused. Such phishing attack compromised the devices that become catastrophic for organizational assets.

Even many companies organize security education awareness program to train the employees so that they can be more careful for suspected mail, but many employees fail to adopt such organizational policies when actually they on work and this led to possible information assets loss.

Volkamer *et al.* (2017) highlighted some human mistake that encouraged phishing attack that are (a) insufficient knowledge about accessed URL, (b) unable to distinguish between trusted and untrusted URL, and (c) users are redirected to implicit URL that makes them unable to see the realistic URL [10].

Problem statement influenced this research to propose a method that not only detects URL based SE attacks, but also protects information assets from the attacker when storing as well as transmit it.

### 1.4.Research Question

The proposed work deal with the following research questions:

1. What are the various techniques are available to detect phishing attacks especially URL based and data protect techniques to protect the organization and individual as on now?
2. How can phishing attacks be detected efficiently and organization assets be protected against social engineering attacks?

## 1.5.Objectives

### 1.5.1. General Objectives

The general objective of this research is to develop URL based phishing attacks detection and protection model to prevent sensitive data.

### 1.5.2. Specific Objectives

To accomplish the general objectives, the following specific objectives will be considered:

1. Exploring related research and literature review that has been done in this area.
2. Exploring and identifying appropriate machine learning approaches for detection of URL based social engineering attacks.
3. Identifying the appropriate features to be used for detecting URL based phishing attacks from the existing SE attack dataset.
4. Proposing detection and protection model, can accurately detect the above phishing attack with better accuracy and protect the information assets.
5. Evaluate, analyze and compared the proposed work against existing work.

## 1.6.Significances of the Study

It is obvious that the usage of internet technologies is dramatically increasing. As a result, on a daily basis, the type and volume of SE attacks are also growing especially phishing attacks. The proposed study explores and addresses not only detection but also provide strong protection mechanism against URL based SE attack so that it is difficult for the attackers to breach the organization and user's sensitive personal data. Additionally, its proposed work will serve as a reference for those who are interested in the area of social engineering attack detection and prevention.

## 1.7.Scope and Limitation of the Study

The proposed study will focus on detect phishing attacks and preventing sensitive data from social engineering attacks. This will enhance the trustworthiness among people against URL based phishing attacks and will encourage people to use their information assets without fear. Proposed work will detect, reduce or mitigate the likelihoods of risk and threats associated with

information assets and that results in a loss in organization and individual. A phishing attack can also be executed over a phone call that is not covered in this thesis work.

## 1.8.Methods

The following methodology is used to fulfill this research process:

### 1.8.1. Description of the Study Area

The study area belongs to network and information security, where the individual or organizational data is susceptible to attack; especially, social engineering environment and information security will be targeted area of this research.

### 1.8.2. Study Subject

The study subject focused on the development of sensitive data protection and detection mechanism toward social engineering attack to protect individual and organizational assets. The study subject includes social engineering and information security & privacy specifically.

### 1.8.3. Study Methodology

The proposed work uses the Design Science Research Methodology (DSRM). This research method allows to start with the problem identification in detection of URL based phishing attack and protecting the organizational or individual information assets. Once problem is identified, dataset is collected that is further preprocessed for reducing the feature. Further machine learning classification algorithms has been applied to detection of attack. Here Decision tree, Random forest, Naïve Bayes and Logistic Regression algorithms has been chosen and implemented over the dataset of 11055 tuples and 30 features that are related with URL based phishing attack. This gives best classifier for detection of attack. Further, data protection model has been proposed that ensures organizational/individual data security. Finally, evaluation measures have been taken to examine that the proposed approaches suitability for detection and protection against URL based phishing attack. Additionally, proposed work is compared with existing solutions proposed by other researchers.

### 1.8.4 Literature Review

In order to achieve the objectives, one as described in specific objectives and satisfying first research question, extensive literature review is taken place on different areas that are considered to be relevant for proposed work. Research papers related to social engineering attacks detection

and mitigation are investigated in detail. This part helps to get knowledge about how to differentiate between the legitimate and phishing identities.

### 1.8.5 Performance evaluation of the Proposed Work

The detection of URL based phishing attack using different machine learning approach has been evaluated to predict phishing attacks. The researcher implemented, evaluated and recommended the best ML approach for detection of URL based phishing attack based on evaluation matrices like precision, recall and accuracy. Further, to protect organizational/individual assets against attacks, proposed encryption/decryption algorithm has been evaluated using performance metrics like key size used, and encryption/ decryption time. Proposed security algorithm is also be qualitatively analyzed against various security attacks. Lastly proposed detection model is compared with existing state of art for its novelty.

## 1.9.Expected Outcome

At the end of this work, the researcher expects detection of URL based phishing attack and protection of personal and sensitive data against social engineering attack with increased confidentiality and integrity.

## 1.10. Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 presents literature review and related work of existing detection approaches and protection approach applied to the problem. In chapter 3 we introduce both our methodology which is phishing feature detection and hybrid cryptography model. We also discuss our machine learning model that we used in our experiments. Also, we explain how this approach can be completely useful in fighting and protect against phishing attacks. In chapter 4 we discuss on experiments and results. We evaluate our proposed approach to conducting different experiments and practical measurement. Finally, chapter 5 concludes the thesis and discusses directions for future work.

# CHAPTER TWO

# LITERATURE REVIEW & RELATED WORK

## 2.1 Introduction

This chapter deals with literature review and existing related articles in the field of social engineering attack detection, mitigation and protection. Specifically, literature review (section 2.1 up to 2.7focused on the background and definition of social engineering attacks, particularly phishing attacks, as well as detection and prevention techniques. Related work (section 2.8) deals with existing state of art work related to phishing attack detection and protection available in the research repositories.

## 2.2 Social Engineering attack

Social engineering in a context of social science defined as a discipline with the objective of encouraging popular beliefs, attitudes, social behavior and action in an extended scale. When social engineering relates with information security, it assists to the attackers to achieve his/her aims by tricking people. It mainly consists of confidence tricks to manipulate users to gain access to critical information assets. According to Wikipedia, social engineering is a confidence trick attempts to deceive a person by first gaining their confidence [11]. The Information Security definition of Social Engineering is also related with the confidence trick. Social Engineering has been defined as follows by a number of information security specialists and academics (as it is in their word):

According to Mann, *"The goal of social engineering is to deceive others into giving up information or performing an action."* [12].

According to Mitnick, *"Manipulation or using influence and persuasion to trick people into believing the attacker is someone he is not. As a result, the social engineer can use people to collect information or persuade them to complete an action item, whether or not technology is used."*[13].

According to Bezuidenhout, *"Social engineering refers to a variety of strategies for obtaining information in order to bypass security mechanisms by exploiting human vulnerability"* [14].

Huber defined, *"The art of social engineering is to attack the weakest link in an information security system: the people who use it"* [15].

Evans defined, *"The purpose of social engineering attacks is to gather a particular amount of data that will be used later in a technological attack"* [16].

According to Foozy,*"The goal of social engineering assaults is to gain direct access to an organization's information or information system by using physical or digital access"* [17].

All these definitions pointed that few things are oblivious. Firstly, above-mentioned writers agreed that the prime target of a Social Engineering attack is the people, which are the weakest link. Second, such attacks are starting phase for classy technical and security attacks. Third thing pointed that social engineering can relate to many other disciplines other than information security.

Finally, according to us, Social engineering attack is defined as *"a harmful activity performed by an attacker to control people, in which the attacker looks out an opportunity to get illegal access to important informational assets and combines human, technical, social, and behavioral aspects"*.

Social engineering attack can be human-centric or device-centric. Human-centric attacks focused directly on people, where attacker apply the attack personally over individual to gain desired information and thus, they can be limited in numbers. But, device-centric attacks use computers and mobile phones with software to harvest information assets and credentials from victims, and they can target a large number of people in a short period of time. Some of the SE engineering attacks are phishing, baiting, pre-texting, tailgating etc. Phishing is one of device-centric SE attack that use Social Engineering Toolkit (SET) to send phishing mails to victim

### 2.3 Social Engineering attack lifecycle

Nowadays, SE attacks are the biggest challenge facing by cyber-society and become major threat for the cybersecurity. These attacks are created differently than usual security attacks [18]. The lifecycle of SE attack is shown in following figure 2.1:

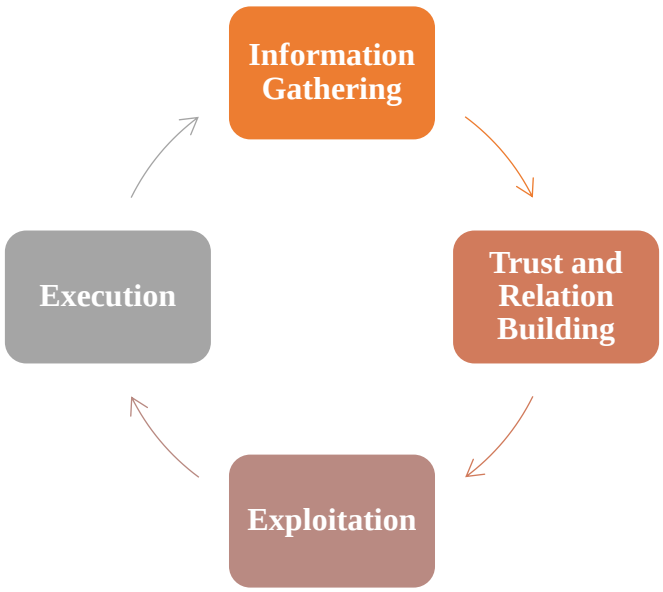



Figure 2.1: Social Engineering attack lifecycle

## 2.4 Phishing attack

Phishing attack is most common cybercrimes that are increasing frequently in cyber society and affecting many online transactions and activities. Phishing attacks are generated by social engineers called phishers with the aim that they deceitfully acquire private credentials and secret from person using emails and phone calls. The phishers subdue the end-user to manipulate them to theft these credentials. They use social engineering toolkit to generate fake website, advertisement, emails and welcome offers. Very common example is spammed email that contain link to win the lottery for sum of money and encourages the victim to click on the given link. This link asks for some credential like social security number or identity of person with account number to deposit the money. Some time they may ask for credit card detail, home address, date of birth or online banking detail. Study conducted by Google says that its software named Google bots detected 9500 fraudulent website per day [19].

The phishing attacks are very difficult to detect even prevent but impossible to stop since most of the time they are unnoticed. Because phishers did not leave any evidence of their intrusion into the target system, the information acquired by them can be used without being detected by existing security mechanisms. For safeguards against such attacks, the user's credentials must be protected from being theft. There should be proper detection mechanism that accurate detect and mitigate such attack and there should be proper security mechanism that can store and transmits the data even after being tricked.

### 2.4.1 Phishing Definition and Detection Methods

As discussed above, the main goal of the phishing attack is to theft the user's credentials such as password, identity, credit card information etc. These attack causes loss of billions of dollars yearly for the business. The definition, classification, lifecycle, and the main methods used for phishing attack are presented in following subsections.

### 2.4.2 Definitions related to phishing attacks

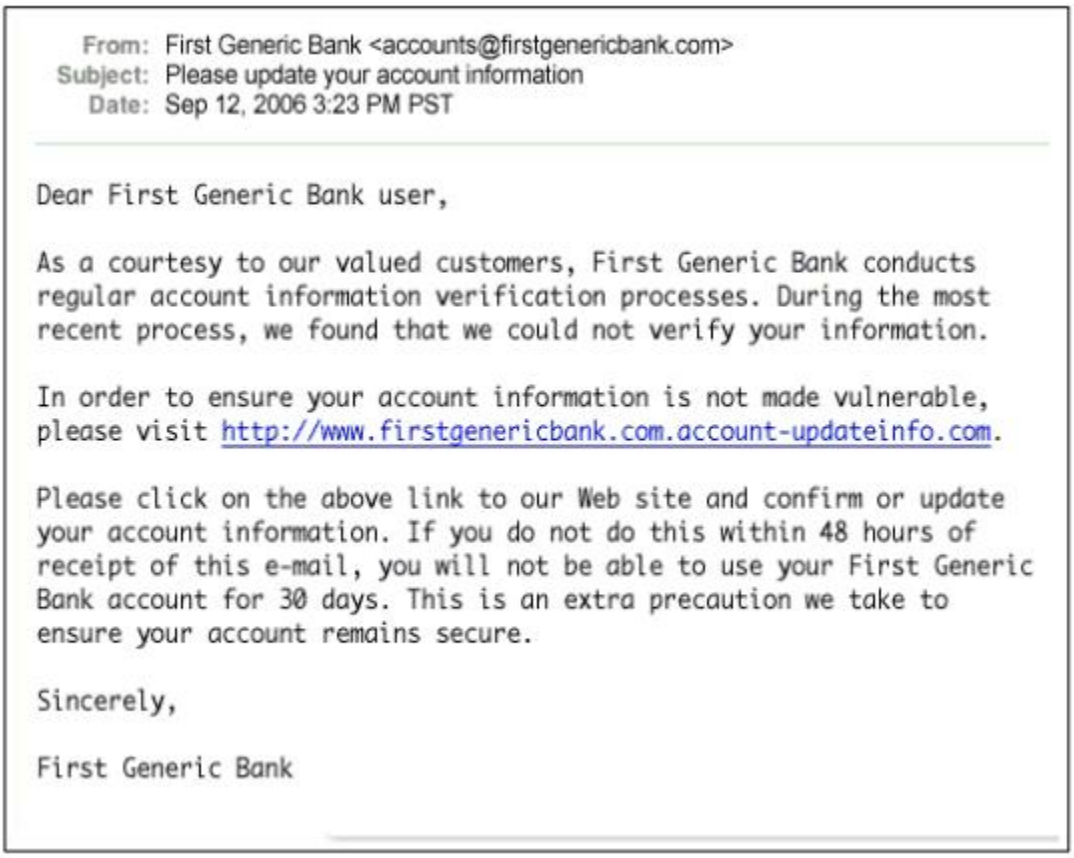
In the scientific literature, phishing terminology has a wide range of definitions, ranging from simple descriptive to very wide, scientific and general definitions. In previous studies, the phishing has not been clearly defined, and is sometimes described using examples [20], while other authors seem to suppose that readers already know what phishing is, or that precise definitions would be too hard for readers to understand [21]. Many authors have proposed their own definitions of phishing, leading to a large number of different definitions in the scientific literature. The most widely known definitions are presented below:

• Phish Tank is one of the most important collaborative clearinghouses for phishing data and information on the Internet. *"Phishing" is defined as "a fraudulent attempt to steal your personal information, usually by email."* [20].

• A longer definition has been proposed by the APWG, which is the most well-known organization coordinating global solutions to cybercrime from the perspectives of business, government, and law enforcement. *"Phishing is a criminal process that uses both social engineering and technical deception to obtain consumers' personal identifying data and bank account credentials," according to the definition. "Spoofed emails posing as real organizations and agencies are used in social-engineering techniques to direct users to fake websites where they are tricked into giving financial information such as user names and passwords."* [21]. The above definitions of the term phishing indicate that each organization has developed their own description of this term.

Lastdrager (2014) tried to find a standard definition of the term phishing based on systematic evaluation of the literature where author gathered 113 unique definitions and combine them together into one definition based on criminal science theory [22]. *"Phishing is a scalable act of deception in which identity is utilized to collect information from a target,"* they said. As pointed

in above mentioned definitions, a typical phishing attack starts by sending an email to the victim as shown in figure 2.2. Where an online Customer received phishing email. This displays the initial stages of a phishing attack.



From: First Generic Bank <accounts@firstgenericbank.com>
Subject: Please update your account information
Date: Sep 12, 2006 3:23 PM PST

Dear First Generic Bank user,

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable, please visit http://www.firstgenericbank.com.account-updateinfo.com.

Please click on the above link to our Web site and confirm or update your account information. If you do not do this within 48 hours of receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,

First Generic Bank

Figure 2.2: Phishing email example[20].

The main components of above mail are described in Figure 2.3. These examples and their annotations are collected from the Phish Tank website [20]. The fake link that the phisher embedded as a trap in this email is for a fraudulent website as shown in Figure 2.4. This fraudulent website is designed by the phisher to convince the recipient that it is a genuine site by appearing exactly as the authorized website. Figure 2.5 shows particular frame where the recipient is anticipated to enter his/her secret credentials, and once he/she entered, the phisher steals the information and further start illegal utilization for their gain.


Figure 2.3: Marked example of a phishing email with its main parts [20]

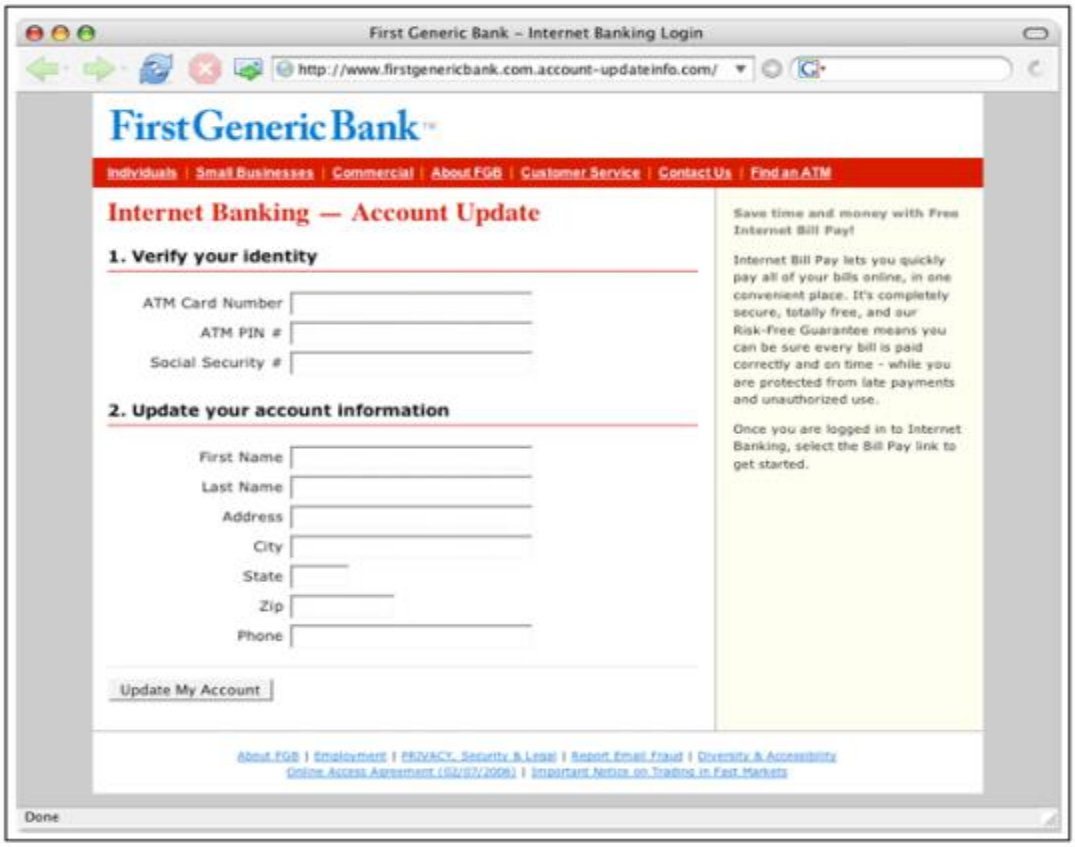



Figure 2.4: Phishing website [20]

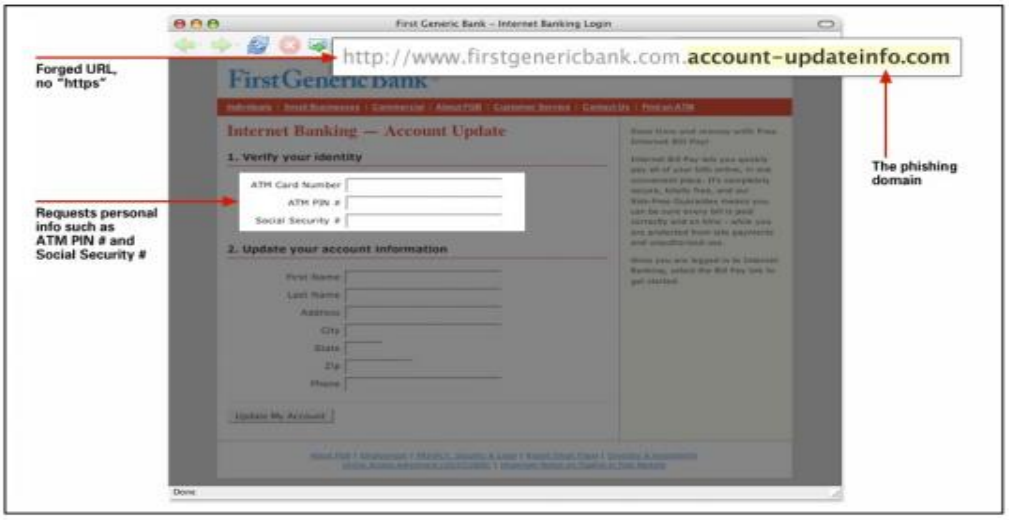



Figure 2.5: Phishing website with annotations [20]

### 2.4.3 Life Cycle of a Phishing Attack

Phishing attacks can be divided into two layers; social engineering and technical subterfuge. Social engineering layer includes attackers, victim, sending fake email, which contains spoofed webpages. Technical subterfuge layer is about spoofed web page. Process of first layer starts by sending spoofed email, which comes from organizations for gathering some sensitive information such as user name, id, password, credit card information etc. Second layer directs the victim to the spoofed web page which visualized very similar to the original page. These layers send the obtained information and get remote access by attackers to victim's computer or original webpage [23].In figure 2.6, the figure is showing the life cycle of a phishing attack.

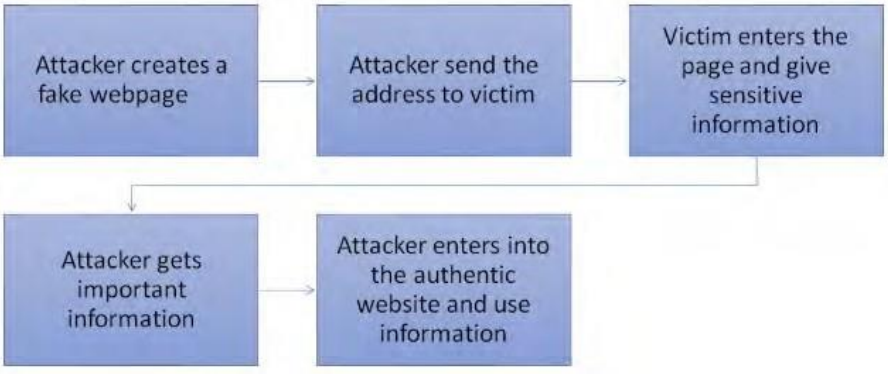



Figure 2.6: Life cycle of a Phishing Attack [23]

## 2.5 Phishing Attacks Detection Methods

Experts have offered a variety of techniques to identify phishing attacks, which can be divided into two categories: traditional approaches and modern approaches. Traditional approach relies on traditional techniques such as authentication or network level protection, while modern approaches utilizing machine learning techniques to detection.

### 2.5.1 Traditional Approach

Traditional methods of detection divided into two classes; (a) the network-level protection, and (b) the authentication protection. The first type of network protection uses filtering techniques such as blacklist and whitelist filters, which prevent phishing by preventing suspect IP addresses or domains from gaining access to the network. In addition, Pattern Matching filters and the Rule-based filters are also other filters which are depended on manually entering and updating static rules for phishing detection [23]. The second class (i.e., authentication protection) provides security on both user and domain levels. For a user-level protection, users will have to provide authentications before sending their messages such as verified email and password [28], while the authentication protection on a domain-level is created for emails servers [23]. Here, researcher is considering only network-level protection technique.

1. **Blacklist Filter**

Blacklist filtering protects networks by categorizing received emails depending on the source MAC address, IP address, or DNS address for which a blacklist has previously been created. These details are extracted from the email's header and compared with a pre-defined blacklist. If any of these data are matched with the list, the emails are rejected. Therefore, this technique filters phishing emails to provide security at a network level. Internet Server Providers (ISP) is the responsible organization of providing and implementing this filter [24]. Since this technique is dependent on third-party service like ISP, sometime it gives poor result and performance. Additionally, this technique does not identify zero-day phishing attacks, because its signatures are not listed in pre-defined blacklist.

2. **Whitelist Filter**

White-list filtering provides network-level protection as well, but unlike blacklists, this technology compares email data to a pre-defined list of static IP addresses of legitimate domains and IP addresses. [25]. In this regard, only emails where data ingredient is matched in the list, are

allowed to access the network for the user's inbox. Email addresses and IP addresses are included in the white-list if they belong to legitimate users or companies who have agreed to add their addresses to this list. Based on this filter, only emails with data matching this list will be classified as authentic, while all other emails will be considered phishing and will be denied access to the network.

**3. Pattern matching filter**

The pattern matching technique filters emails based on specified patterns and its term frequency. This includes words, text strings, and character sets written in the email's content, subject, or sender. The filter searches complete email for these specified patterns to classify the email into phishing or legitimate. Although this technique provides protection at a network level, it still provides some invaluable and false results due to the huge number of received emails which may include banned words or text strings but shall not be prevented [26].

### 2.5.2 Modern Approach

This approach is also referred at automated approach which utilizes automated classifiers to detect the phishing attack and it is based on machine learning techniques. These classifiers work based on examining different features rather than the servers and filters to detect phishing or legitimate mails [27]. One of the modern methods using machine learning is URL-based detection that detects the false URL based on URL features. URL-based detection performs faster than other above techniques. Even this method works over zero-day phishing attack that is the important concern in cyber-security societies. This even reduces the workload and detection time as compared to above mentioned techniques.

Machine Learning (ML) is a branch of computer science that aims to develop and apply algorithms that automatically extract meaningful patterns or other information from a set of observed data, with the ultimate goal of characterizing known data in order to make intelligent inferences on unknown data. The observed data is sometimes referred to as a training data set, while the unknown data is referred to as test dataset. An instance may contain an individual bit or set of bits. The instance is defined by its features, which are often specified specifically by the ML expert but can also be inferred by an algorithm. Each instance is a member of a distinct class. An algorithm "learns" to differentiate between one or more groups based on variations in the distribution of features within classes. There are several phases to machine learning. 1) Data

collection and preprocessing, 2) feature extraction and evaluation, 3) classifier training, and 4) testing and evaluation are the phases. ML is closely linked to mathematical approaches that allow for the extraction of data, the discovery of patterns, and the drawing of conclusions from it.

Although there are many types of machine learning algorithms, they can be divided into three categories: supervised learning, unsupervised learning, and reinforcement learning. For the computer security area, a number of researchers applied ordinary machine learning algorithms. These includes decision trees (DT), support vector machines (SVM), Bayesian algorithms, k-nearest neighbor (KNN), random forest (RF), association rule (AR) algorithms and principal component analysis (PCA).

Proposed work utilizing Logistic Regression, Decision tree, Naïve Bias and Random forest for detection and evaluation of URL based phishing attacks. The detail of these algorithm is as follows:

**1. Random Forest (RF)**

Random Forest is a machine learning classifier that can be used for classification and regression. It creates decision trees from randomly selected sets in training samples, then aggregates the results by averaging or majority voting. It increases precision and decreases overfitting [28] [29]. Bagging is used to build a Random Forests with random attribute selection. To improve efficiency, it uses a divide-and-conquer strategy (ensemble mechanism). The system in random forest blends numerous random subsets of trees. The average, or weighted average, of the individual outcomes is used to measure the total result. The accuracy is determined by a calculation of the classifier's dependency and the power of the individual classifiers, and they help to solve the problem of decision tree overfitting.

Random Forest is a classification algorithm that employs an ensemble of multiple decision trees. Each decision tree makes its own independent predictions about the data, and the prediction with the most votes become the model's actual prediction thanks to the majority voting principle.

The concept of "wisdom of the crowd" underpins the influence of ensemble classifiers. We can eradicate errors caused by individual trees if we can create a forest of trees that all make unrelated decisions. The low correlation factor is critical because without it, we'd just keep making the same decision over and over.

Using two strategies, bagging and feature randomness, we can ensure a low correlation between the classifiers in random forests. In general, decision trees are responsive to the training data; even minor differences in the input data will result in drastically different tree structures. Bagging takes advantage of this property by training each tree on a random sample with replacement rather than a fixed collection of training samples. Feature randomness makes it easier to choose which features to split on since only a subset of the features are considered during a split.

**2. Decision Trees (DT)**

One of the most widely used classifiers in classification and regression is the decision tree classifier. It divides the training data until it hits a leaf node, which in classification is a marker. Unlike Random Forest, the Decision Tree classifier constructs a tree using the entire training dataset [30]. The aim is to learn basic decision rules from data features to build a model that predicts the value of a target variable. Nodes and arrows make up a graphical model of classification called Decision Trees. The Root is the root node from which the Decision Tree is started. Each node in the network has an "If-then" law, a class, and a function, and uses arrows called edges to connect to the next one. The terminator is a leaf node at the end of the decision tree. The internal nodes of the tree are bounded by the root and terminating nodes, and the tree may contain one or more classifier stages.

Many decision tree implementations, such as ID3, C4.5, and others, are available (C5.0). The ID3 model, which employs entropy information as a heuristic function to identify the objective, is one of several algorithms for creating decision trees that have been presented. In 1992, this algorithm was enhanced to the C4.5 algorithm. In this way, the decision tree would generate sub-trees, with each node in the tree having a parent node (except for the root) that leads to a child node (except for the terminating node), and the tree ending with the terminating node (leaf node) that represents the final solution of the proposed problem [31].

Decision trees are popular predictive models in machine learning, as well as in statistics and data mining. A decision tree is a supervised learning system that is non-parametric in nature. A predictive model is built by inferring rules from feature vectors in data points. "Decisions" are represented by internal nodes, while expected groups are represented by leaf nodes. The majority of algorithms build a decision tree from the top down. An algorithm starts at the root node and

recursively chooses the "right" decision, that is, a function + a criterion, After then, the remaining instances are split into child nodes until the node is pure or there are no more features to choose from. A node is said to be pure if it only includes instances from one subclass, in which case it is called a leaf node.

**Decision trees have the following advantages**:

- They are simple to understand and execute, and they are similar to a human-like approach to solving classification problems.
- Explaining why a particular instance belongs to a projected group using only basic Boolean logic is a clear explanation of outcomes.
- The ability to see the tree.
- Scalability to high-dimensional feature vectors and large-cardinality instance sets. Despite the fact that the worst-case time complexity is quadratic in terms of the number of features and cases, the complexity in practice is linear.

**The following are some of the disadvantages of using a decision tree:**

- Building an overly complex tree that over fits the training data. This lack of generalization translates to poor test data results.
- If a particular category dominates the dataset, a biased tree is built. By using a balanced training dataset, this problem can be avoided.
- Instability is an issue. Even with minor changes to the data, a major difference in the resulting tree can be seen.

### 3. Logistic Regression (LR)

Because of its easily interpretable and realistic effects, logistic regression is a commonly used technique. Since it is based on statistical data and uses a generalized linear model, this model is useful for predicting binary data (0/1 response). Despite its simplicity, this approach has three flaws. First, it needs more statistical assumptions before it can be used. Second, it works better for variables that have a linear relationship than with those that have a complex relationship. Finally, the completeness of the data affects the accuracy of the prediction rate [27].

The coefficients assigned to each function in logistic regression models are also (relatively) intuitively interpretable, which is a useful property. A positive coefficient for a function indicates

that it increases probability, while a negative coefficient indicates that it reduces probability. The size of the coefficient of an individual feature is related to the intensity of the feature (the amount it increases or decreases the probability). The coefficients can then be used to decide which features are most useful to the model. Logistic regression is a discriminative probabilistic model with a binary output that is commonly used. When the training size is near to infinity, logistic regression outperforms the Naive Bayes model [32].

**4. Naive Bayes (NB)**

Naive Bayes methods are a set of supervised learning algorithms based on Bayes' theorem and the "naive" assumption of conditional independence between any pair of features given the class variable's value. The Bayes theorem is used to construct a generative probabilistic model in machine learning. Because of its simplicity, it is most commonly used in classification areas such as text classification and spam detection. Its characteristics are distinct from one another. The naive Bayes algorithm is one of the most ancient machine learning algorithms. These algorithms are based on Bayes' probability theorem, with the "naive" assumption that given the class variable, all pairs of features are conditionally independent of each other. Of course, in real-world situations, this presumption is rarely accurate. However, for classification problems such as spam filtering, naive Bayes algorithms have proven to be an effective method. Bayesian classifiers outperform more complex methods in terms of speed. The fact that Bayes model probability estimates are considered to be inaccurate is a drawback for certain tasks that depend on them. The classification is based on Bayes' Theorem, and independent predictors are assumed. To put it another way, this classifier would conclude that the presence of unique features in a class has nothing to do with the presence of any other function. If there is a dependence between features or on the existence of other features, each of these will be treated as an individual contribution to the output's likelihood.

This classification algorithm works well for large datasets and is simple to implement [33].

## 2.6 Preventing Information Assets

The proposed research on social engineering attack is divided into two parts: Phishing attack detection and protecting the organizational or individual assets against social engineering attack. Detection deals with finding the URL based phishing attack and protection covers the method an organization/individual can adopt to prevent SE attack. The security of informational assets become a big issue, since Cybercriminals always try to theft information from organization for

their fun and profit. Thus, companies must be alert in protecting their informational assets. By and large, protection classified under information security, which protect the informational assets by means of preserving confidentiality, integrity, availability and liability of informational assets. Following figure 2.7 shows levels of information security for protecting organizational/individual assets.

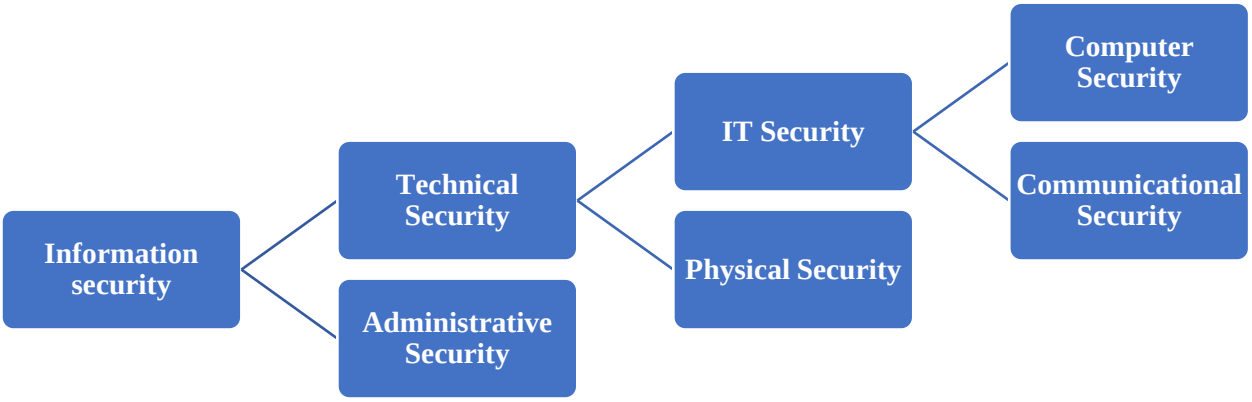



Figure 2.7: Levels of Information Security.

Social Engineers have the ability to do a lot of harm to the victim. This harm may be social, financial, or reputational in nature. It is more important than ever to consider what steps can be taken to deter, mitigate, and contain the damage that a Social Engineering attack can potentially cause. As a result, this section outlines the most popular forms of social engineering attack protection methods that organization/individual adopt to protect their information assets against potential SE attack. These methods are influenced from above shown levels of information security with reference to protecting SE attack.

### 2.6.1 Physical Security

Physical security meaning covering the perimeter of the organization against attack. This include both physical entry and exit points of the organization including network facility room and datacenters where informational assets are stored and serviced. Only properly approved staff should have access to these properties, which must be secured and controlled. Physical security must be strong and it must be checked for any vulnerability periodically, so that security system must be up to date. Physical security may include usage of CCTV cameras to capture illegal activity within premises or it may be instructed and trained the employees that they should not

plug in unauthorized USB/flash derive and other digital devices found within the premises because some time attacker spreads such device to use, which contains harmful program. Furthermore, employees must be self-vigilant and must inform about any distrustful behavior to the organizational security system, even it is minor in perception. If adequate physical controls are implemented within the organization, it might be possible that company may prevent considerable SE attacks. If not, company always welcome the attacker by keeping its door open for illegal access for attacker who will get free access to intrude the company's premises.

### 2.6.2 Personnel Security

Users/people are easily available and exploitable by the SE attacker to gain the access of network, system or data. Thus, they are more vulnerable for SE attack. Personal security is related with empowering employees of the organization so that they can be able to protect their asset. This requires training and education workshops with expert and leaders, regarding protecting their own credentials. For example, people should be trained for creation of strong login-id/password, periodically changing them, encourage them to use strong rotational policy for their credential, not to reveal their credentials to others over internet or phone call etc. It should also be mandatory for the organization to find background of newly appointed employee to check their involvement in criminal activity.

### 2.6.3 IT Security

IT security is a defensive measure to SE attacks that employs a series of hardware and software technologies to mitigate the danger of an attack. This includes anti-virus anti-malware system, intrusion detection/prevention system with updated versions and email-filtering service using firewall and strong encryption methods to guard the organizational information assets. Nowadays encryption techniques are increasing utilizing within organizations as industry standard and regulation for securing communication as well as stored data to ensure the CIA triad [34]

The proposed approach uses cryptography as a security solution to protect organizational information assets from SE attacks. In this work hybrid cryptographic algorithm is used that employed AES and RSA algorithm in combination. Next section discusses the background of proposed hybrid cryptographic algorithm.

## 2.7 Cryptographic background of proposed encryption algorithm

Cryptography is a way of encoding secret informational assets in order to keep them safe from attackers while in storage and transit [35]. Many researches has been implemented information security using a hybrid method which combines encryption algorithms to make them hybrid. Cryptographic algorithms are mainly categorized into symmetric and asymmetric algorithms. This distinction is based on number and type of keys used in the algorithm. Symmetric encryption uses only one and same type of key of encryption as well as decryption. This key is referred as Private Key. While Asymmetric encryption method uses two different keys, one of encryption and other for decryption. These keys are referred as Public and Private key respectively[36]. Sometime symmetric and asymmetric encryption algorithms are combined together to provide strong security and referred as hybrid cryptography. Nowadays majority of researchers are using hybrid way of encryption to protect the informational assets[37]. Because the length of the key determines the cryptosystem's strength, having a large key allows the key domain to be used in a variety of ways, removing the algorithm's internal weakness.

Symmetric encryption method is shown in following figure 2.8, where the user (named Emma in the figure) encrypts a message X using symmetric encryption algorithm that uses K; a key; to generate the encrypted text Y. This encrypted text is called cipher text that transferred over insecure channel toward destination entity (named David in the figure). The receiver utilizes the same algorithm for decryption and key K to decrypt the cipher text Y into original plain text X. Since, the cipher text looks like random arbitrary bits, the attacker (name Carl in the figure) cannot be able to understand about the original text.

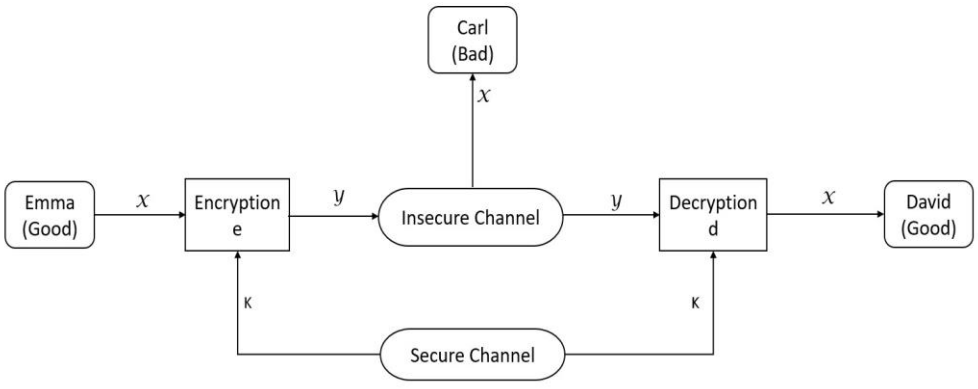



Figure 2.8. Symmetric-key cryptosystem.

Symmetric encryption standard comes into two varieties named stream cipher and block cipher. Stream cipher is applied over the bit streams of any length while block cipher split the original text into blocks of fixed size [38] as shown in figure 2.9.

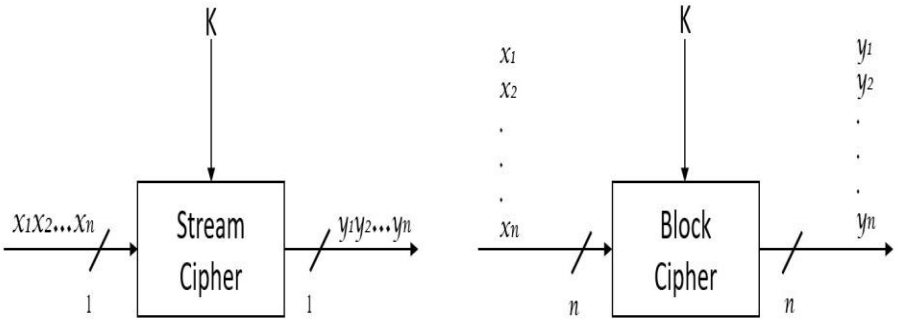



Figure 2.9 Principles of encrypting n bits with stream and block ciphers.

Block cipher algorithms often use block sizes of 128 bits or 64 bits, similar to the AES and DES encryption algorithms [39].

Public key cryptography is another name for asymmetric encryption. This approach employs two keys: one is the public key, which is used by the sender to perform out the encryption process, and the other is the private key, which is used by the receiver to perform out the decryption process. This cryptographic method does not require pre-shared key or digital signature as need in the symmetric key algorithm. Hence provide strong security mechanism when information/secrete data is transferred over the channel. The process of asymmetric encryption is shown in following figure 2.10, where sender (named Bob in the figure) maintained the list of public keys all the receivers in form of ring. Bob used public key of receiver (named Alice in the figure) to encrypt the plain text using encryption algorithm (named RSA in the figure). The cipher text generated through RSA is transmitted over the insecure channel toward the receiver. The receiver uses its own private key to decrypt the cipher text or to generate the plain text back from cipher text.

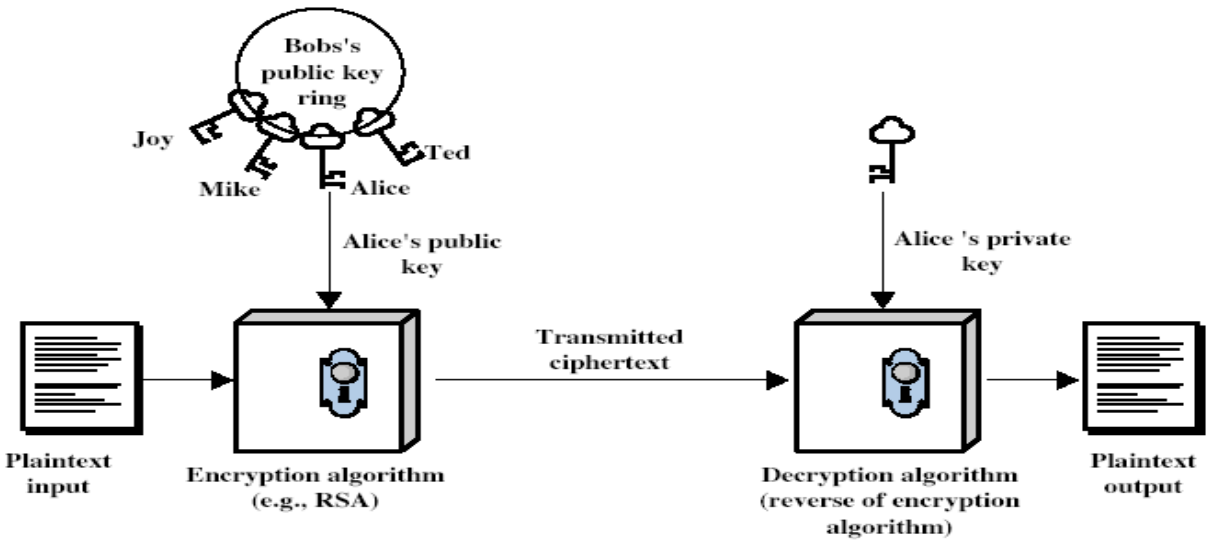



Figure 2.10. Asymmetric-key cryptosystem.

Proposed work combined Advanced Encryption Standard (AES) algorithm as symmetric algorithm and Rivest Shamir Adleman (RSA) algorithm as asymmetric algorithm to propose hybrid cryptographic algorithm. The detail of AES and RSA is shown in next section.

### 2.7.1 AES algorithm

AES algorithm is a symmetric block cipher algorithm which take the plain text of any size and convert it into 128 bits blocks. Further blocks are processed into various round inside the algorithm [40]. AES algorithm have three variation based on key size used and called AES-128, AES-192, and AES-256, where 128, 192 and 256 are key size used inside the algorithm respectively [41]. AES algorithm is executed in various rounds, for example in AES-128 algorithm, 10 rounds are executed to convert the plain text into cipher text. Similarly, AES-192, and AES-256 executes 12 and 14 rounds respectively. Each round executes some operations like byte-wise transformation using XOR function, byte substitutions and permutations. Each block of plain text (sized 128 bits) is referred as State and arranged into 4 X 4 matrix. These states are processed in 10 rounds to generate confusion and diffusion of data that further converted into cipher text after ten rounds [39, 40, 41]. For a ten round (128-bits AES) iteration, nine rounds are similar with four transformations namely SubBytes, ShiftRows, MixColumns and Add RoundKey but the tenth round has only three transformations less the MixColumns. AES encryption/decryption process is shown in figure 2.11. The high-level algorithm for AES encryption is given below: -

```
NormalRound_AES (DataState, RoundKey[j])
{
        SubstituteBytes (DataState);
        ShiftingRows (DataState);
        MixingColumns (DataState);
        AdditionRoundKey (DataState, RoundKey[j]);
}
LastRound (DataState, RoundKey [NumRounds])
{
        SubstituteBytes (DataState);
        ShiftingRows (DataState);
        AdditionRoundKey (DataState, RoundKey [NumRounds]);
}
```

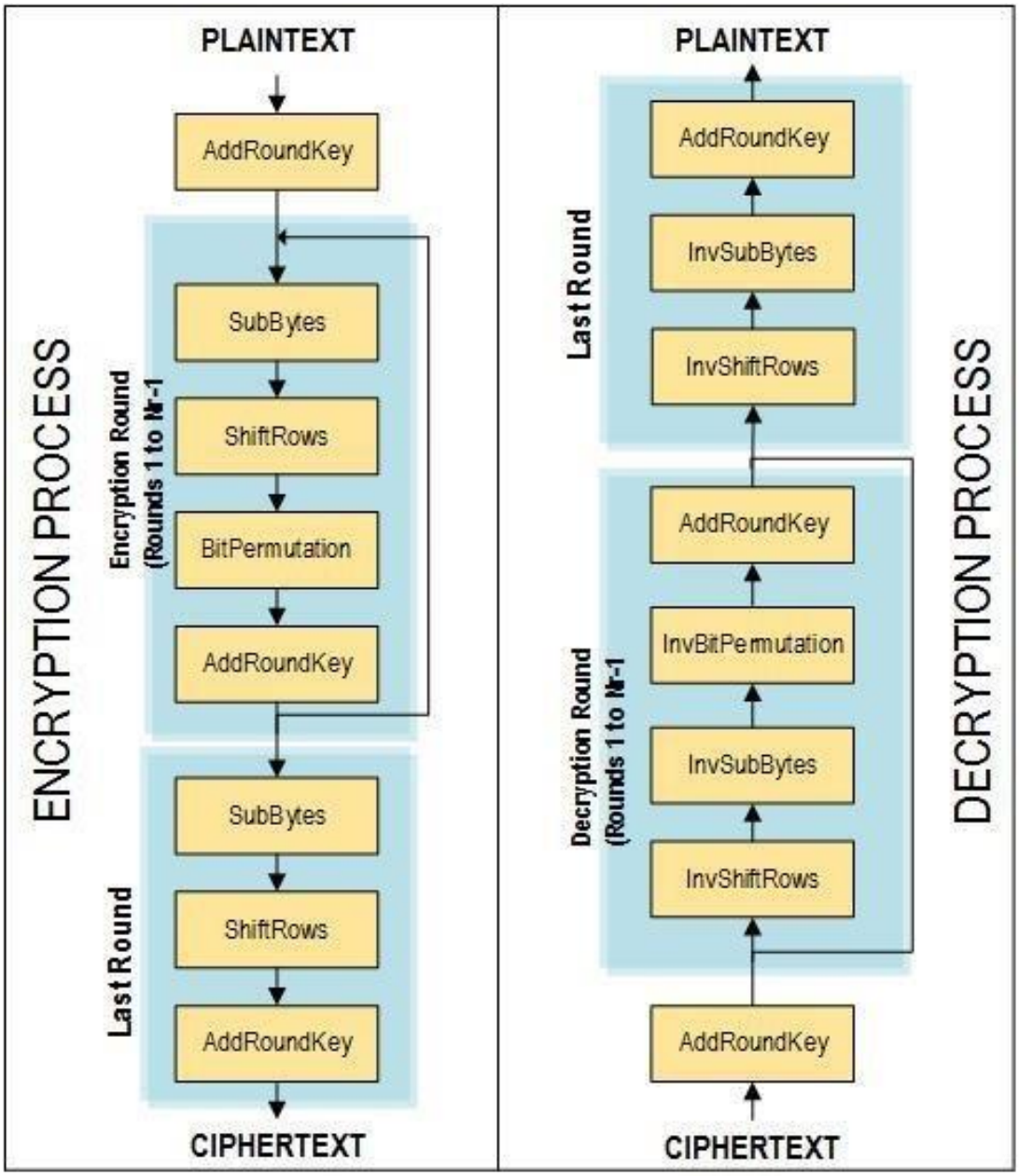



Figure 2.11: AES encryption/decryption process

### 2.7.2 RSA algorithm

The RSA algorithm is public key cryptographic method that utilize public and private key to encrypt and decrypt, plain and cipher text respectively. RSA algorithm is proposed by Ron Rivest, Adi Shamir and Leonard Adleman at MIT [43]. RSA is most widely used encryption standard because it depends on the difficulty of factoring of very large integers. Key length used in RSA is always power of 2. For normal application, it is recommended to use 1024 bits key

size, but it is advised to use large key size 2048 bits to increase security level. However, it is not strict required, i.e. any key length can be used but it must be power of 2 and not be less than 128 bits [43]. Majorly RSA has two large steps: (a) Key Generation, and (b) Encryption/Decryption process.

**[A] RSA Key Generation**

Every participant in the network must generate their own Public and Private Key pair using following steps:

1. Let p and q be large prime numbers, randomly chosen from the set of all large prime numbers.
2. Compute n = p x q.
3. Choose any large integer, e, so that: <e ; a public key>
   **GCD (e, ϕ(n)) = 1** <where ϕ(n) = (p-1)(q-1) >
4. Compute $d = e^{-1} \pmod{\phi(n)}$. <d ; a private key>
5. Publish key pair e and n {e,n} to every user in network. *Keep p, q and d secret.*

**[B] Encryption/Decryption**

Assume sender 'A' wants to send something confidentially to receiver 'B':

- A takes M, <M is message>
- Computes C = Me mod n where (e, n) is B's public key. Sends C (cipher text) to B
- B takes C,
- finds $M = C^d \bmod n$, where (d, n) is B's private key

This whole process is shown in following figure 2.12.

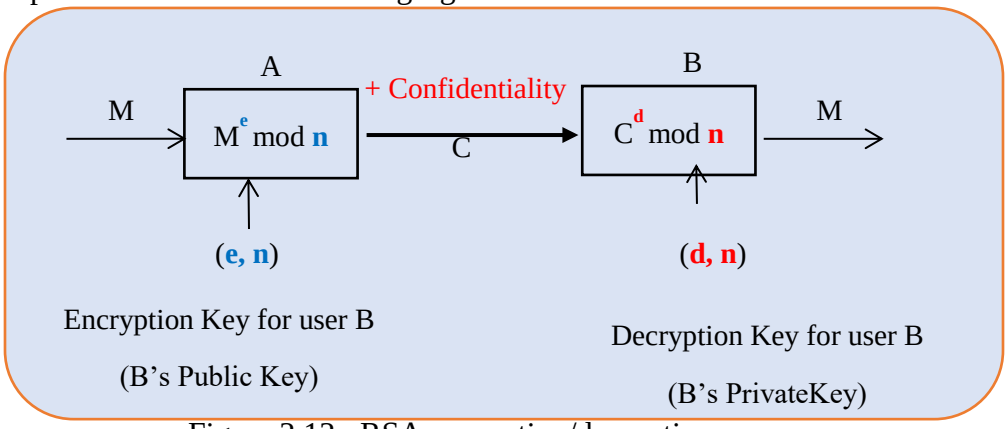



Figure 2.12: RSA encryption/decryption process

## 2.8 RELATED WORK

Many researchers have proposed different detection and prevention techniques to detect the threat launched with phishing attacks. This section examined some of the related studies that helped the researcher understand the present level of study on social engineering attack detection and protection.

### 2.8.1 Phishing Attack Detection

Hason N. *et al.* (2020) proposed a vigorous feature selection mechanism to create better malicious domain detection models. Author collected 5000 genuine URLs and 1350 destructive URLs into their dataset. Further they have created hybrid feature set that blends commonly used features with novel engineering features to demonstrate resistance to adversarial example attacks. Logistic Regression (LR), Support Vector Machine (SVM), Extreme Learning Machine (ELM), and Artificial Neural Networks were used in the evaluation (ANN). The proposed feature set, according to the author, improves classifier performance from 90.2 percent to 98.4 percent [44].

Rahman *et al.* (2020) presented the performance of various machine learning algorithms for detecting URL-based phishing attacks was evaluated. According to the authors, inappropriate selection of ML algorithms and feature set can impair the efficiency of an anti-phishing system. In this work, author selected machine learning classifier named k-NN, Decision tree, Support Vector Machine, Extremely Randomized Tree and Gradient Boosting Tree GBT. Authors used three publicly available dataset with multiple features for evaluation purpose. Performance has been evaluated used various performance matrices including confusion matrix, precision, recall etc. Author claimed that they got 98% best accuracy in Extremely Randomized Tree [45].

Dan & Gupta (2019) proposed novel and better social engineering attach detection and data protection model, which can be used by the employee of any organization. This model is used not only to detect the social engineering attacks, but also to protect their files containing sensitive information and data from attackers. The proposed model was designed to work on two layers not only to detect which is attack detection and data protection layer. In the attack detection layers, they used decision tree which contain a set of questions that would help the individual on detecting whether the requisite is trying to deceive or lure him or herself in to reviling sensitive information. The question was designed to support an individual in making a proper estimate or

predicting whether the requester is attempting to deceive him or her or perform any social engineering attack on him or her [46].

Jain A.K. and Gupta B.B. (2018) presented PHISH-SAFE anti-phishing system that is based on machine learning algorithm. The proposed detection algorithm based on URL features. Author used 14 features from URL for detection phishing or non-phishing websites. Author used SVM and Naïve bayes algorithm as machine learning algorithm for classification of websites as legitimate or illegitimate. For detecting phishing websites, the author claimed 90 percent accuracy using the SVM algorithm [47].

Hossein Shirazi *et al*. (2018) presented detection of phishing website using the large number of training features and types of datasets. Author suggested that the domain name is much better and useful method in detection of phishing websites. Author has proposed designed features using binary and non-binary valued feature to model the relationship of domain name as visual and statistical to the key elements of phishing webpages. Author has collected the dataset of 1000 ranked website and 1000 phishing website from the alexa.com and phishtank.com respectively. Their learning model trained only with 7 features on sample dataset and achieved 98% true positive rate and 97% classification accuracy. Author claimed 99.7% accuracy in detection of unknown live phishing URLs [48].

Chin, T. *et al.* (2018) proposed "Phish Limiter" which is phishing detection and mitigation method using Software Defined Network (SDN). The proposed method employees Deep Packet Inspection (DPI) approach using store & forward, and forward & inspect modes on SDN switching device which running Open V Switch (OVS). In his work, phish Limiter uses score called PLS for every incoming packet and predefined threshold value on OVS, which further computed and maintained to determine which mode to be used among SF and FI based on the comparison of these two scores. The author used ANN classifier model to identify and classify the incoming packet as phishing or non-phishing category[49].

Mouton, F. *et al.*(2015) proposed the SE attack detection mechanism (named SEADMv2) for detection of attacks using series of questionaries' called here state that requires answer in either 'yes' or 'no'. These questions stated whether the replier faced the scenarios of social engineering attack or not. Author's proposed mechanism detected textual as well as verbal SE attacks. Author developed Android based application that implemented proposed detection mechanism

SEADMv2 and called Social Engineering Prevention Training Tool (SEPTT). Proposed mechanism is tested based on the reply of twenty subjects for getting knowledge about whether subject get trapped by social engineering attack or not. It is claimed that proposed android application rid out people from malicious SE attack [50].

Abu-Nimeh (2007) examined and compared various machine learning algorithms for their accuracy in phishing and non-phishing emails with 2889 tuple dataset and 43 features. Author has compared Logistic Regression, Classification and Regression Trees, Bayesian Additive Regression Trees, Support Vector Machines machine learning algorithm for their performance evaluation. Author has claimed that random forest performs best an error rate of 7.7% [27].

M. Loock. (2005) reviewed the characteristics and features of phishing attacks, and then advised actions and responsibilities that individuals and organizations should take to prevent phishing assaults. Although author identified the features of SE attack, but also, they presented mitigation method. This paper presented very old information and as it is known that phishing is evolving rapidly in the society [51].

### 2.8.2 Prevent Social engineering attacks

Nowadays, social engineering attacks becoming applicable in different area of fields such as banking, e-commerce, health care, aviation, social media and several real-world applications by collecting a user or victims' personal information. Social engineering attacks technique has recently got a lot of attention from the research community, as a result a number of social engineering attacks, techniques, studies and results have been published in research literature worldwide. Some of them are as follows:

Thakur, T. N., & Yoshiura, N. (2021) presented novel anti-phishing model to protect mobile banking system called AntiPhiMBS-Auth model to mitigate the security attack like phishing attack, MiTM attack and replay attack. Proposed model worked as application to prevent the mobile banking users from phishing attack. In this method author distributed some secret credential like application id, token number, and a unique id when user installed the application in the mobile and it worked as password, so whenever transaction is happened over mobile app, all transactions are encrypted using those keys and whenever phisher tried to get the information from user, phisher need that credential to understand the received information. Author used process Meta language (PROMELA) for success verification of transaction using PROMELA

Interpreter called SPIN. Author claimed that this model is error-free and banking system can implement verified system for protecting against phishing attack [52].

Hossain, S *et al.* (2020) presented mechanism to detect and prevent phishing attack detection. For prevention against phishing attack author discussed Anti-phishing Tools like e-bay toolbar and Spoof Guard software, list-based protocol including black-list and white-list approach, two-factor authentication and user training. Finally they compared the all the protection method to distinguish the advantage and disadvantage of those methods [53].

Dan & Gupta. (2019) Proposed novel and better social engineering attach detection and data protection model, which can be used by the employee of any organization. This model is used not only to detect the social engineering attacks, but also to protect their files containing sensitive information and data from attackers. The proposed model was designed to work on two layers not only to detect which is attack detection and data protection layer. In the attack detection layers, they used decision tree which contain a set of questions that would help the individual on detecting whether the requisite is trying to deceive or lure him or herself in to reviling sensitive information. The question was arranged in a way to help an individual in making a correct guess or predict whether the requester is trying dupe him or her trying to perform on him or her any social engineering attack.

The data protection layers are used in their model to protect sensitive data and information from the attacker. If an individual has a sense of doubt on the requester or fire something unusual the individual can transfer his or her file cloud plat form in an encrypted. This would prevent the attacker in the accessing the original data even after getting information from the individual. In their cryptography process, they used a symmetric cryptography mechanism for encrypt or decrypt the data. They also divide the original message in to three separate message components and store in three separate files. Then, they apply symmetric key encryption of AES, DES and RC-2 encryption method for each divided message; respectively, to increase the level of security, then the keys of encrypted files stored together in a single file and they encrypt the keys file by using list significant bit (LSB)-based stenography algorism for improving the security level. Finally, the images will be sent to the individual e-mails id and they also revise process for decryption [46].

Conteh, N. Y., and Schmick, P. J. (2016) explained the relevance and the role of social engineering in network intrusions and cyber-theft. In this paper authors recommended few preventing methods and solutions for the social engineering threat and vulnerabilities. Paper discussed some vulnerabilities like human behavior, human impulses and psychological predispositions that influenced though social engineering. Author discussed various SE attack like phishing, pretexting, baiting and tailgating etc. As a proposed solution for protection, author kept human element as a central and proposed multi-dimensional technical solutions that includes security policy, education and training, network guidance, audit and compliances, technical procedure like IDS/IPS and physical protection. To secure the organizational network from social engineering attacks, the author presented the usage of a defense in depth structure with IDS/IPS, firewall, demilitarized zone, web filters, and virtual private network [54].

Singh A.P. (2011) presented anti-phishing method as a prevention of phished attack that relied upon dynamic watermarking technique. Author proper three tier model which works in three modules called Registration process, login verification process and website closing processing. In this work user has asked for additional information like watermark image, its fixing position and secret key at the time of user's registration and further, these credentials of particular user had been changed at per login. During each login, a user will verify the authentic watermark with its position and decide the legitimacy of website [55].

Other than above most of the researches has demonstrated that both industry and academia have contributed significant effort to deliver end-user training to enable them in understanding of the relevance of cybersecurity, especially in anti-phishing context [56], [57], [58], [59], [60]. All these researches emphasized that phishing-based education for organizational employee needs to be considered as a method to combat such threat. It is shown in their results that human behavior is most important to protect against phishing attack that can be changed by provide proper training and education to end-user. All authors claimed that member's phishing avoidance behavior after post-test assessment has been improved. A. G. Arachchilage (2015) [61] presented their findings on the design and development of a mobile game prototype as an instructional tool for teaching and assisting digital users in avoiding SE phishing attacks. These previously published researches stressed that people are more vulnerable for phishing mail. So, training and education, previous background of employees and technical support must be implemented within the organization to protect their informational assets.

### 2.8.3 Cryptographic algorithms literature review

Joshna. (2016) presented a fair comparison of four symmetric key algorithms, DES, 3DES, AES, and Blowfish. Round block size, key size, encryption/decryption time, and CPU time are all factors in the comparison. The blowfish algorithm was found to be more suited than the AES algorithm[62].

D. P. Timothy and A. K. Santra. (2017) Presented designing a new security method by using a hybrid cryptosystem, for data security. The proposed model uses both symmetric and asymmetric cryptography algorithm in which Blowfish dealt with data confidentiality whereas, RSA dealt with authentication. Additionally, the method also combined Secure Hash Algorithm–2 for data integrity. They did comparison between MD 5 and SHA to show why they selected SHA with different parameters and also, comparison of SHA functions (i.e., SHA0, SHA1 AND SHA2) with algorithm and variant. The result shown that, proposed method provides high security on data transmission over the internet using SHA-2 algorithm. The combination of symmetric and asymmetric algorithm provides efficient data security over the network [63].

A. Alrawais et al. (2017) presented a key exchange protocol based on Cipher Text Policy Attribute-Based Encryption (CP-ABE). To create secure communications among the participants, they combined CP-ABE and digital signature techniques to realize confidentiality, authentication and verifiability and access control. Their main contribution in this work was developed protocol for encrypted key exchange based on CP-ABE that combined encryption and signature and then examined the security protocol under different attack scenarios, evaluated the performance and efficiency of the protocol with message size and communication overhead. Paper also implemented and compared the protocol with a certificate-based protocol. For implementation authors used Python under OS X 10 operating system and used Charm cryptography library that wraps the Stanford Pairing-Based Cryptography (PBC). They evaluated the efficiency of the protocol with security and performance. They confirm the proposed protocol correctness and feasibility [64].

Various research presented hybrid approach for presenting cryptographic algorithm. Some of the researcher used RSA and Digital signature algorithm [66], while other block cipher like AES and RSA [67].

Onyesolu and Ogwara (2016) designed a hybrid encryption algorithm using two symmetric encryption algorithms namely, 3DES and AES together [65]. Rani and Kaur explained about two cryptosystem called AES and Elgamal. Further author combined them in a hybrid algorithm. Author reported that proposed hybrid cryptographic technique experienced lower encryption and decryption time and increased the system throughput. The Cryptographic algorithms play a very important role in network security [66].

V. Kapoor and Rahul Yadav (2016) described about network security and says that the network data is prime to secure by network and service providers. In this work data is secured by encryption technique when it is transmitted. Author proposed hybrid encryption technique for ensuring data security during transmission and further implementation and results are recorded. The proposed cryptographic method ensures the highly secure cipher generation technique using the RSA, DES and SHA1 technique. The result concluded the efficient and improved cipher text during comparative performance analysis [67].

All the above research pointed out that hybrid algorithm provides more secure and convenient method for securing data that is either in transmission or storage. According to some of the studies mentioned above, hybrid encryption has proven to be a more secure cryptosystem when it comes to preventing attacks on informational assets held in an organization's data.

## 2.9 Summary

This literature review has shown that phishing is a challenging type of attack that is hard to defend against, even with the highest security solutions, since it targets human weakness to attain its goal. Phishing is becoming more complex along with developments in communication channels, and many different phishing types are appearing. This chapter suggests a wide range of researches over social engineering and especially phishing is possible. However, to keep the research within manageable proportions, this thesis focuses on detecting phishing attacks and provide protection to information asset. This chapter has described various formal definition of social engineering and defined the how SE attack behaves in its lifecycle. Further this chapter discussed specially about phishing attack and its lifecycle. Further various phishing attack detection approach including traditional as well as Machine learning algorithms has been discussed in section 2.5. Further literature related to prevention of information is discussed that researcher explored from literature review. This includes physical, personal, IT security. Section

2.7 discussed about cryptographic background of encryption algorithm. This includes background of AES and RSA encryption algorithm that can play important role in security of information assets. Section 2.8 explored selected related work on phishing detection, prevention and cryptography.

# CHAPTER THREE
# MATERIALS AND METHODS

## 3.1 Introduction

This chapter discusses the numerous materials that were used and the methods that were established in relation to the proposed research. The material outlines the technical requirements for implementation of the proposed work, such as the working environment for the proposed work. Methodology deals with processing steps or mechanism used to implement the proposed work. This chapter also discusses various performance metrics for the evaluation of proposed work.

## 3.2 Methodology Used

To evaluate the suggested solution for the problem stated in Chapter 1, the proposed work used Design Science Research Methodology (DSRM) that is widely used in Computer Science. The proposed methodology is divided into two phases: detection phase and data protection phase for phishing attacks. The detection phase is used to detect phishing attacks, while the data protection phase shows how to protect information assets against phishing attacks. For detecting the phishing attack, the detection phase used several machine learning methods such as Random Forest, Decision Tree, Naive Bayes, and Logistic Regression. In the proposed work, researcher has considered only URL based phishing attacks. Every individual algorithm has been implemented and evaluated based on given performance metrics. Further, best algorithm has been chosen to detection. Phishing URLs are identified using detection algorithms based on their content. The data protection phase uses hybrid cryptography algorithm to safeguard sensitive data or informational assets against social engineering attacks. By mixing asymmetric and symmetric methods, a hybrid RSA and AES cryptography model is employed for this purpose. Following subsections details about URL based dataset and its preparation for processing.

### 3.2.1 Understanding URLs

URL is very important to see the pattern in phishing attack. That's why it must be known how the URL is intersected inside. This requires detailed understanding of the various parts of the URL. A typical URL consisted of five important parts as shown in the following figure 3.1:

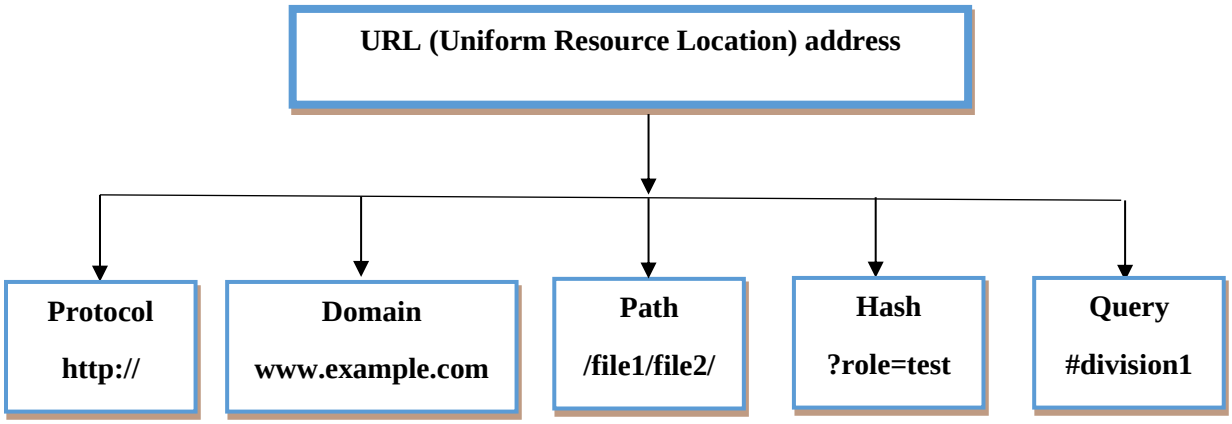



Figure 3.1: components of A URL

This first component of the URL is Protocol that defines the rules for transmitting data. The domain, which is made up of numerous elements, is the second part of the URL. The “www" prefix, which stands for World Wide Web, is frequently found in the first part of a domain. The website's name is then given following a dot. In domain name after a dot, organizational type (for example, com, edu, gov, etc.) is added. Sometime it shows the country code also (like et, in etc.). The path details indicate website's sections and pages that are found in the third part of the URL.

The fourth section consists of a query that refers to a section of a page and preceded by a hash sign. It redirected the website to other resources like other portion like footer or sidebar. Mostly it contains id of a HTML element. Finally, the Query section used as an internal search and sends any additional information that was submitted along with the page request. Mostly it followed by ‘?’ mark.

### 3.2.2 Dataset description and feature extraction

The URL data was taken from the UCI Machine Learning Repository [68], which was released in 2015. There are 11055 URLs in total. That are maintained in single CSV file that delimited by tabs and encoded in UTF-8. We have extracted the features of URL in feature extraction phase and total 30 features are taken in experiment as initial input. That are further reduced into 15 after feature selection.

### 3.2.3 Dataset Pre-processing

The pre-processing occurs after data collection is included in this section. Pre-processing is act of converting data into a format that is more suitable for the machine learning algorithm being used. Feature extraction extract of elements of URL, and feature selection gives important features out of available features that influenced higher accuracy of detection. This section goes over the many processes of pre-processing. Feature extraction is a key stage in the process of converting raw data into various features.

In the proposed work, main goal is to use the extracted features to determine if the URLs are phishing or legitimate. Feature are extracted in preprocessing, where the textual URLs were sent to the feature extractor program, coded into python language. This program accepts URL as the input and generate output as binary value. Program contains set of 'if statements' that checks the URL elements features based on predefined URL-based feature and that classifies the URL elements into either phishing, suspicious or legitimate. Some of extracted features with its binary value is shown in the table 3.1 below. Here, features have binary values of 1, 0 and -1, where 1 is used for URL phishing feature, -1 is used for URL legitimate feature and 0 for suspected URL. Details of every features has been discussed in next section. The extracted feature values are passed to the classifiers as input. The classifiers are given a structured dataset for detecting phishing or legitimate URLs. Proposed work used four classification methods namely Random Forest, Decision Tree, Naive Bayes, and Logistic Regression. Detail about these algorithms is discussed in chapter two. The classifier can now determine whether the requested URLs is a phishing URLS or Legitimated URLs. Extracted feature collected from dataset are represented in a form of table (row and column) for sake of understanding, where each row represents one tuple of the dataset which contains number of features in various columns for that one URL tuple.

Mostly next step of preprocessing deal with any missing or incorrect data that arises throughout the data collection process. In the proposed work, since features are extracted based on python program, there were no any missing value found in the dataset.

Table 3.1: Structured Dataset with URL features and its binary values after feature extraction.

| id | having_IP_Address | URL_Length | Shortining_Service | having_At_Symbol | double_slash_redirecting | Prefix_Suffix | having_Sub_Domain | SSLfinal_State |
|---|---|---|---|---|---|---|---|---|
| 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | -1 |
| 2 | 1 | 1 | 1 | 1 | 1 | -1 | 0 | 1 |
| 3 | 1 | 0 | 1 | 1 | 1 | -1 | -1 | -1 |
| 4 | 1 | 0 | 1 | 1 | 1 | -1 | -1 | -1 |
| 5 | 1 | 0 | -1 | 1 | 1 | -1 | 1 | 1 |
| 6 | -1 | 0 | -1 | 1 | -1 | -1 | 1 | 1 |
| 7 | 1 | 0 | -1 | 1 | 1 | -1 | -1 | -1 |
| 8 | 1 | 0 | 1 | 1 | 1 | -1 | -1 | -1 |
| 9 | 1 | 0 | -1 | 1 | 1 | -1 | 1 | 1 |
| 10 | 1 | 1 | -1 | 1 | 1 | -1 | -1 | 1 |

Above collected dataset is divided into four major classes of attributes/features[68] that are as follows:

1. Address based attributes
2. Abnormal-based attributes
3. HTML and Java Script-based attributes
4. Domain-specific attributes

All these classes are now shown and explanation is given in following tables 3.2, 3.3, 3.4 and 3.5.

Table 3.2: Address-Based Feature

| Feature Name | Explanation |
|---|---|
| IP Address | It is a phishing website IP Address rather than a domain name. |
| URL length | Malicious material can be hidden behind a long URL name. It is deemed suspicious or phishing if the URL is longer than the typical length of a URL. |
| TinyURL | TinyURL is a service that shortens URLs. When you click on the shorter URL, user will be forwarded to the main page. TinyURL links are considered phishing websites because they |

| | |
|---|---|
| | can lead to a bogus website rather than a legitimate one. |
| Having “@” symbol in URL | Because the section related to the @ sign is usually skipped by browsers, it is avoided in real addresses. |
| Using “//” symbol | The symbol "//" is used to link to another website. If the sign is used after HTTP or HTTPS, considered genuine and if after the first protocol declaration considered phishing. |
| Having “-” in domain name | The “-” sign is absent from the majority of genuine URLs. If the domain name contains the letter "-,” considered phishing. |
| Dots in domain | To append a sub-domain to the domain name, it is needed to add a dot. If there are more than one subdomain, consider it suspected, and anything more than that will be flagged as a phishing site. |
| HTTPS | Because most legitimate websites utilize HTTPS and have a trusted certificate, the age of the certificate is quite important. |
| Domain expiry date | A legitimate URL domain name usually has a longer expiration date. |
| Favicon | A website's favicon is a graphic image. It can redirect users to dubious sites if it is loaded from an external domain. |
| Using unimportant ports | Phishers can take advantage if a URL that has several unneeded open ports. |
| “HTTPS” on domain | A phishing website is identified by the presence of the letters "HTTPS" in the URL's domain name. |

Table 3.3: Abnormal-based attributes

| Feature Name | Explanation |
|---|---|
| Request URL | If webpage have many external URL or contents of another domain, considered as suspected or phishing. |
| Using tags | Same as above, if more tags are included in webpage, phishing may be there and declared as suspected or phishing. |
| Links in <meta>, <script> and <Link>tag | If these tags contains many external links, it is considered either as suspected or phishing. |
| Server Form Handler (SFH) | If it is blank or empty, phishing is considered. If the user is redirected to another domain by SFH, considered suspected. |
| Submitting Information to Email | After submitting the information over webpage, if it is redirecting to user E-mail rather than to server, it is considered as phishing. |
| Abnormal URL | If the URL is not contain the identity, considered as phishing. |

Table 3.4: HTML and Java Script-based attributes

| Feature Name | Explanation |
|---|---|
| Website forwarding | If website is redirecting many times, it is suspected. |
| Status Bar Customization | The “onMouseOver” event used to alter the status bar in the website. This hides the false URL and display the true URL to trick users. If such kind of event is available, considered as phishing. |
| Disabling Right Click | Generally, attacker disable the right click event of mouse so that user cannot be able to check the source code. If it so, considered as phishing. |
| Pop-up Window | If popup window with text box/field is available on the webpage, considered as phishing. |
| <iFrame> tag | iFrame tag is used to specify inline frame to load external elements in the website. Phishers generally used it to hide |

| | |
|---|---|
| | the malicious code. If it is found considered as suspected. |

Table 3.5: Domain-specific attributes

| Feature Name | Explanation |
|---|---|
| Age of Domain | If the domain is older than 6 months, considered as genuine otherwise considered phishing, since phishing website intended to create for short time. |
| DNS record | DNS record is an instruction that is available in the DNS server and provide knowledge about the IP address associated with domain and can be associated with website. If it unavailable in website, considered as phishing. |
| Website Traffic | Website traffic means number of users visiting the website and it is measured in visits or sessions. This helps to decide whether it is phishing or not. Highest visit website mostly does not have probability to be a phishing website. |
| PageRank | Every website is assigned a value called rank of website. If website is so important, its rank value is higher. If any website does not have rank value, considered as phishing. |
| Google Index | Every year Google assigned the index to URL. If website is malicious, then it does not have google index and considered as phishing. |
| Links pointing to webpage | If webpage host belongs to top phishing IP/domain, considered as phishing. |

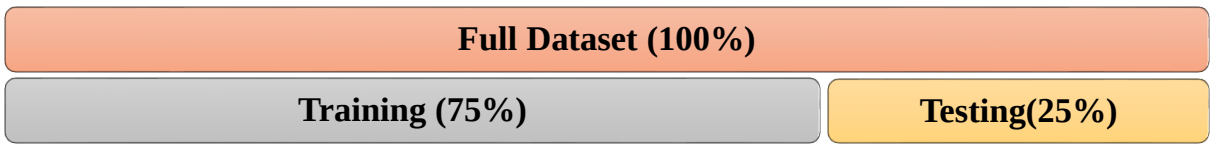
Further, feature selection technique is applied over initial dataset. This is done because some features allow ML algorithm to execute with better efficiency (i.e., in terms of time and space) that make them more effective. For this purpose, researcher used Recursive Feature Elimination method, or RFE in short as feature selection algorithm. Basically, there are two types of methods used for feature selection: Wrapper and filter method. Wrapper model approach uses the method of classification itself to measure the importance of features set, hence the feature selected depends on the classifier model used. While the filter method scores or rank every feature individually and select if it produces the largest (or smallest) score. Wrapper methods generally

result in better performance than filter methods because the feature selection process is optimized for the classification algorithm to be used. RFE is wrapper type of feature selection method, where different machine learning algorithms are wrapped individually with this method in the program to produce the feature. Here researcher given discussed four ML algorithm with RFE individually to select the feature. RFE executes by searching a subset of features starting from all feature over training and testing dataset and iterate many times until the wanted number leftovers. In the proposed work, researcher has taken 15 most important features that shown in chapter 4.

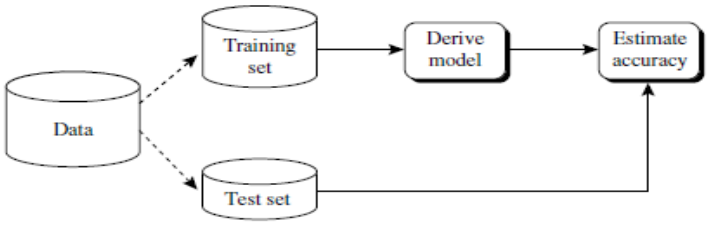
### 3.2.4 Models Training

In this step, the given dataset is randomly partitioned into two independent sets, a training set and a test set. Typically, the training set contains three fourth of the dataset, while the test set obtains the remaining one-fourth. The model is created using the training set. The model's accuracy is then estimated with the test set. The estimate is pessimistic because only a portion of the initial data is used to derive the model as shown in figure 3.2.

In the proposed work, the dataset is partitioned into 75 percent as training samples and 25 percent as testing samples before the Machine Learning model is trained. The input URL dataset is classified after processing using used model as phishing (1), suspicious (0) and legitimate (-1). The dataset in this study was trained using supervised machine learning classification techniques such as Decision Tree, Random Forest, Naïve Bayes, and Logistic Regression. All of these are executed over the training dataset, and further the test dataset is used to evaluate the model.




(a)




(b)

Figure 3.2 (a) Training and testing dataset division. (b) Estimating accuracy

Following table 3.6 shows the description of dataset after division:

Table 3.6: Dataset division in Training and Testing with number of phishing and benign URL.

| **Original Dataset** | **Training Dataset (75%)** | | **Testing Dataset (25%)** | |
|---|---|---|---|---|
| 11055 | 8291 | | 2764 | |
| | **Phishing URL** | **Benign URL** | **Phishing URL** | **Benign URL** |
| | 4653 | 3638 | 1504 | 1260 |

### 3.2.5 Model validation and optimization

Since, it is impossible to predict the accuracy at primary level, so it is needed to validate the performance of classifier, which is a vital step for data analysis. The validation is achieved using the Python's module called model selection. This is important to validate that whenever new data is included in the system, it is classified correctly or not, i.e. classifier classifying the result consistently or not. This is because it does not indicate how well the learner will generalize to a dataset that has never been seen before.

The first validation occurs during the model training phase, when the entire dataset is split into two sections, each of which is trained and tested separately. This is achieved in the proposed work using fit () and predict () that comes under GridsearchCV() function to perform the training and testing datasets in a sequence. Every ML classifier includes training multiple models on the given dataset and select one that outperforms. But this is not sure that particular model is the best or not. This gives the chance for improvement. As a result, researcher used 10-fold cross validation method to validate, evaluate and compare the adopted machine learning algorithms in proposed work. For this, researcher used model_selection.KFold() function of python. In particular, researcher used stratified 10-fold cross-validation because most of the researcher in previous works as well as literature reviewed recommended it for estimating accuracy (even if computation power allows using more folds) due to its relatively low bias and variance. Following figure shows the general k-fold cross validation method, in which dataset is divided into k folds and one of the folds is used as test set at one iteration out of k, while rest k-1 folds are used to train the model. As shown in figure 3.3, this method is repeated until every fold out of k has been used as a test set.

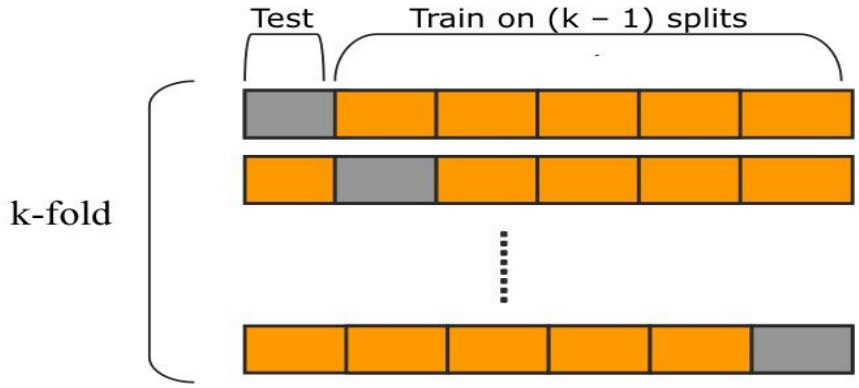



Fig 3.3 k-fold cross validation

### 3.3 Working Environment

#### 3.3.1 Working Environment Phishing detection

The implementation tool used for URL-based phishing Attack detection is python in proposed work. The dataset was initially converted to.csv format for detection. The file was then examined using selective methods using machine learning utilizing the python tool. Python is further used for implementing prevention technique to protect the informational asset.

Python is a multipurpose programming language that can be used for a diversity of applications and tasks including machine learning, web development, data science, software prototyping, and so on. It can freely use and share even for commercial purposes, because it is free and open-source and simple to learn. Python's syntax is both basic and attractive syntax. Python programs are significantly easier to read and write than programs written in other languages such as C++, Java, and C#. Python programs can be moved from one platform to another and executed without modification.

In the proposed work, researcher used Scikit library (commonly referred as ‘sklearn’) that is free ML library for Python. It supports various machine learning algorithm like Random Forest, Decision tree, Naïve Bias, Logistic regression, SVM, k-NN etc. It also integrates various other libraries like NumPy and SciPy for numeric and scientific calculation. It is provided pandas library to import and explore the dataset. Sklearn provided various tools for machine learning and data or statistical modelling. Some of the functions used in implementation of proposed work are read_csv() to import the dataset for processing, train_test_split() to divide the dataset, GridSearchCV() for parameter turning for getting optimal values of accuracy for given

algorithm, fit()to fit the given algorithm over given training dataset, predict() to returns or predict the label of data value based on trained model, accuracy_score() for performance evaluation etc.

For Hardware point of view, following configuration has been used as shown in table 3.5

Table 3.7. Hardware tools used in proposed work

| **Operating System** | **Windows 10 Pro** |
|---|---|
| **Processor** | Intel(R) Core(TM) i3-3110M @ 2.4GHz, 2.4 GHz |
| **Installed Physical Memory (RAM)** | 4.0 GB |
| **System Type** | x64-based PC |

### 3.3.2 Working Environment for Protection

The implementation tool used for data protection against phishing Attack is also python. For protection, researcher has used crypto module of python. Further, other modules like Random, AES, RSA has been imported from this module. To create the key for encryption and decryption various functions are used for example generate_key() function is used to generate AES key, while get_public_key() and get_private_key() functions are used to get RSA public/private key pair. To encrypt and decrypt the data, encrypt (), decrypt () functions have been used that contains other function for its working. The hardware configuration is same as detection mentioned in table 3.7.

## 3.4 Evaluation metrics

This section includes metrics for determining how good or “accurate” a classifier is at predicting the dataset tuple's classification model. Using training data to derive a classifier and then estimate the accuracy of the resulting learned model can result in misleading overoptimistic estimates due to overspecialization of the learning algorithm to the data. Instead, it is better to measure the classifier’s accuracy on a test set consisting of class-labelled tuples that were not used to train the model.

True-Positive (TP), False-Positive (FP), True-Negative (TN), and False-Negative (FN) are the four main metrics used to assess the effectiveness of predictive models. The following are the definitions of these metrics:

1) TP – classifier correctly detects a benign URL
2) FP – classifier incorrectly detects a benign URL
3) TN – classifier correctly detects a malicious URL
4) FN – classifier incorrectly detects a malicious URL

These terms are summarized in the confusion matrix of Figure 3.6. The confusion matrix is a useful tool for analysing how well the classifier can recognize dataset tuples of different classes. TP and TN outcomes when the classifier is getting things right, while FP and FN outcomes when the classifier is getting things wrong (i.e., mislabelling). Figure 3.4 shows a graphical representation of these binary classifier metrics.

| | | **Condition** | |
|---|---|---|---|
| | | Present | Absent |
| **Test** | Positive | True-Positive | False-Positive |
| | Negative | False-Negative | True-Negative |

Figure 3.4. Structure of confusion matrix for binary classifier

On the basis of above metrics, following evaluation measures has been considered in the proposed work:

**[a] Accuracy:** On a given test set, the accuracy of a classifier is the percentage of test sets correctly classified by the classifier.

$$Accuracy = \frac{TP+TN}{P+N} \qquad (1)$$

This is also known as the classifier's overall accuracy rate in most literature, and it refers to how well the classifier detects tuples from different classes. When comparing classifiers, just because

one classifier's accuracy is higher than the others doesn't indicate it's the best. Depending on the system, there are additional evaluation measures to consider.

**[b] Precision:** can be conceived of as a metric for precision (i.e., what percentage of tuples labeled as positive are actually such).This metric can be computed as:

$$Precision = \frac{TP}{TP+FP} \qquad (2)$$

**[c] Recall**: is a condition for completeness (what percentage of positive tuples are labeled as such). If recall like sensitivity, it's because they're the same thing (or the true positive rate). This metric can be calculated as follows:

$$Recall = \frac{TP}{P} \qquad (3)$$

### 3.5 Proposed Approach

The proposed algorithm has two phases: URL based phishing attack detection phase and Data Protection phase that are described in subsequent sections as follows:

#### 3.5.1 URL based phishing attack detection Technique

In this phase, the preprocessed dataset is given to different classification algorithms. Namely, Random Forest, Decision Tree, Logistic Regression, and Naive Bayes. This individual classification algorithm develops their own models and the dataset, the experimental environment and testing option is the same for all algorithms. Individual algorithm has been evaluated the performance based on performance metrics. Based on the outcome of the evaluation, the comparison of is done. Finally, the best classifier is selected for the classification of URL based phishing attack and benign. The order of execution of program is shown in following figure 3.5.

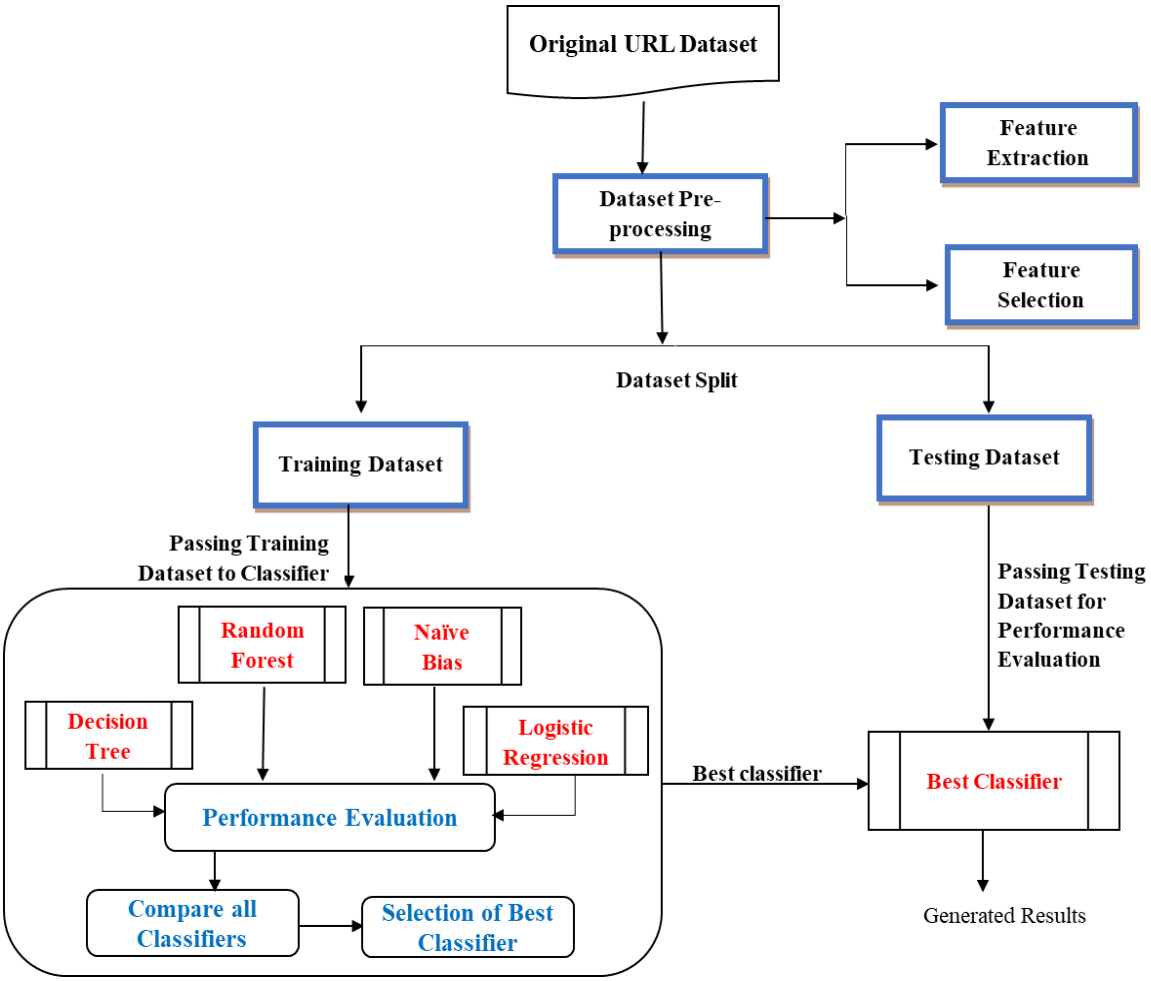



Figure 3.5: Workflow for proposed detection phase

First, a URL-based dataset is collected from the UCI machine learning repository, which has 11055 rows and comprises both malicious (phishing URLs) and benign URLs (as indicated in the above picture). Then dataset is converted into .CSV format and then important features has been extracted and assigned them binary values (1, 0 and -1). Further, Feature selection is executed, that give 15 best features out of 30 that are further preprocessed by assigning them binary values (1, 0 and -1). Now the dataset is divided into training and testing dataset with 75 and 25 percent division. In next step, the training dataset is passed to individual machine learning algorithms/classifier for classification. The results of individual classifier are further evaluated. On the basis of result obtained, best classifier is selected. Now, best classifier is chosen, which is given test dataset for testing and validation and finally results are obtained based on evaluation matrices. The same process is shown as algorithm below:

1. *Input dataset D*
2. *Preprocess the dataset*
   - *Feature extraction*
   - *Feature selection*
3. *Apply Random Forest algorithm on the preprocessed dataset*
   - *Evaluate the performance*
4. *Apply Decision Tree algorithm on the preprocessed dataset*
   - *Evaluate the performance*
5. *Apply Naïve Bayes algorithm on the preprocessed dataset*
   - *Evaluate the performance*
6. *Apply Logistic Regression algorithm on the preprocessed dataset*
   - *Evaluate the performance*
7. *Compare evaluation performance of Step 3, 4, 5, 6*
8. *Take the best classification based on evaluation performance from step 7 and use as a proposed classifier.*

### 3.5.2 Proposed Data Protection Model

The second phase of proposed work deals with protection of sensitive information asset from the attacker. This proposed model will protect, if the user has a sense of distrust for the requesting entity or if user is doubting something suspicious. Then after providing basic information about asset, the employee/individual stores the files into an encrypted format. It will prevent the attacker from accessing the assets in their original format, even getting some basic information about assets. For this, the proposed work proposes the Hybrid encryption/decryption method that combines AES and RSA algorithm to provide an adequate level of protection. This Hybrid encryption/ decryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. If the requester is authorized person, then he/she will be able to decrypt the information using his/her secret credential. Following figure 3.6 shows a conceptual model for an organization's data protection in order to secure an asset from an attacker.

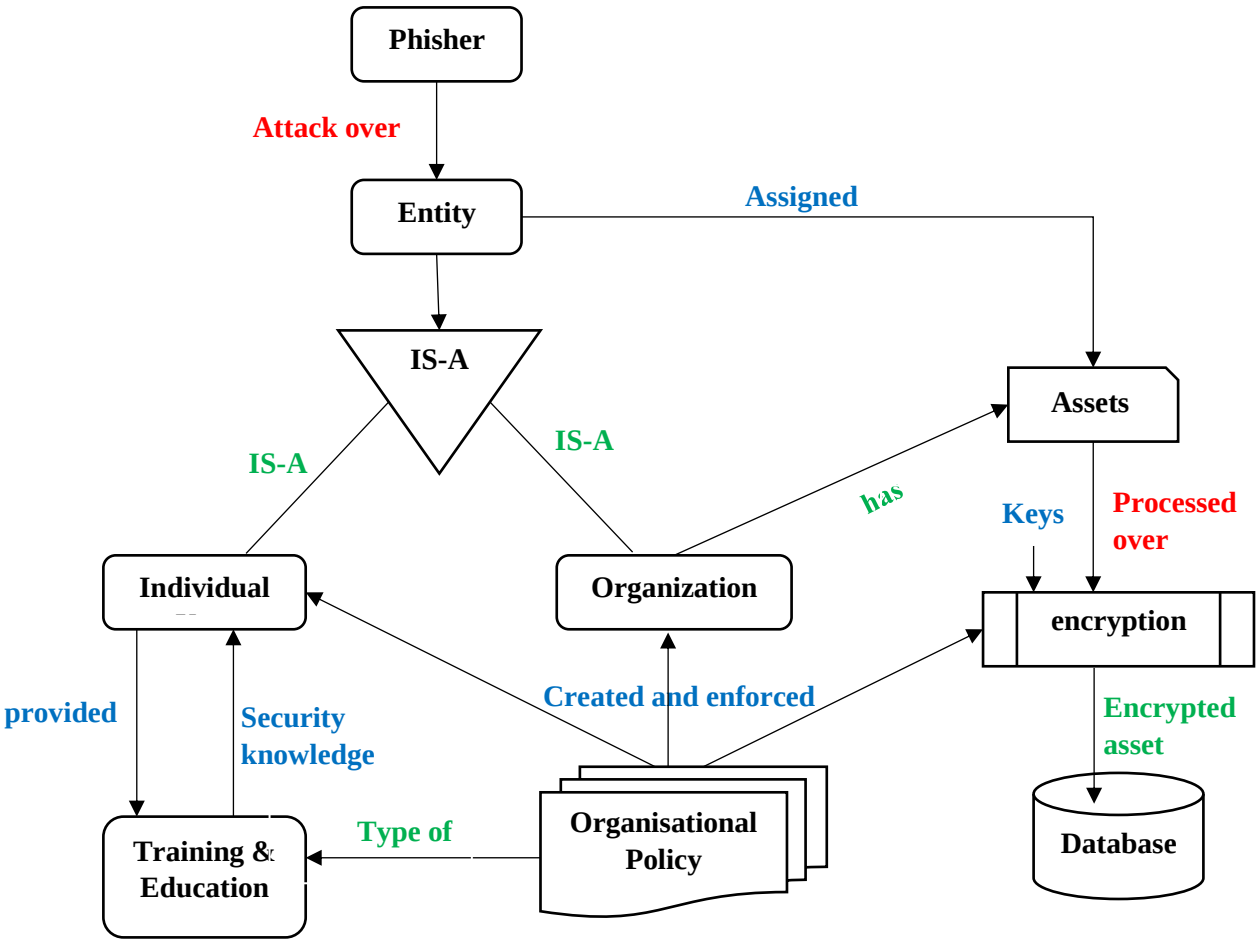



Figure 3.6: Conceptual model for data protection

As shown in the figure 3.6, phishers attempt to attack any entity, whether it is an individual user or an organization. The organization has many organizational assets that are assigned to individual users. The organization has a number of data protection policies that are applied across the organization as discussed in chapter 2 in section 2.6 for preventing information assets. One of the policies is training and education that is provided to every user. Additionally, the organization employs technical solution like encryption/decryption to encode and store the assets in a secret form. This requires the use of symmetric/asymmetric keys applied over the encryption/decryption method. The detailed process of the proposed technical solution has been shown in Figures 3.7 and 3.8 that demonstrate the encryption and decryption process respectively.

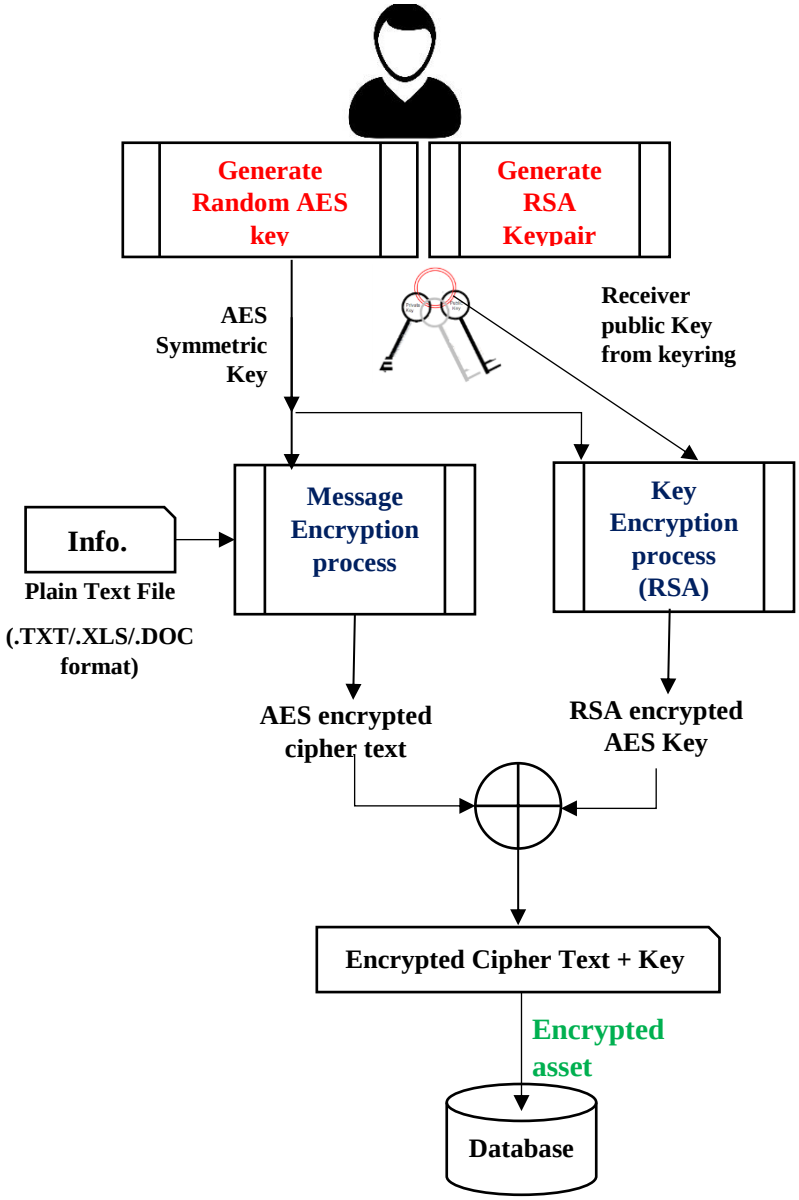



Figure 3.7: Hybrid encryption using AES & RSA

Figure 3.7 shows the process of hybrid encryption, in which first of all user machine generates symmetric and asymmetric key pair. Symmetric key is generated randomly for every message, while asymmetric key pair is generated once that are further used for encryption and decryption process. When user has any message to encrypt to it first generate random symmetric key that is given to AES algorithm with generated symmetric key. This process generates the cipher text. For security of symmetric key, proposed work utilizes the RSA encryption method. That take the symmetric key as input and generate cipher version of key. Now both cipher message text as well RSA encrypted AES Key is concatenated together and stored in to the database. The

decryption process shown in figure 3.8 first of all take the message from database and parse it into two parts that are AES encrypted cipher text and RSA encrypted AES Key. Now firstly cipher symmetric key is decrypted to get plain AES key. Then this key given as input to message decryption process with AES encrypted cipher text to get plain text message.

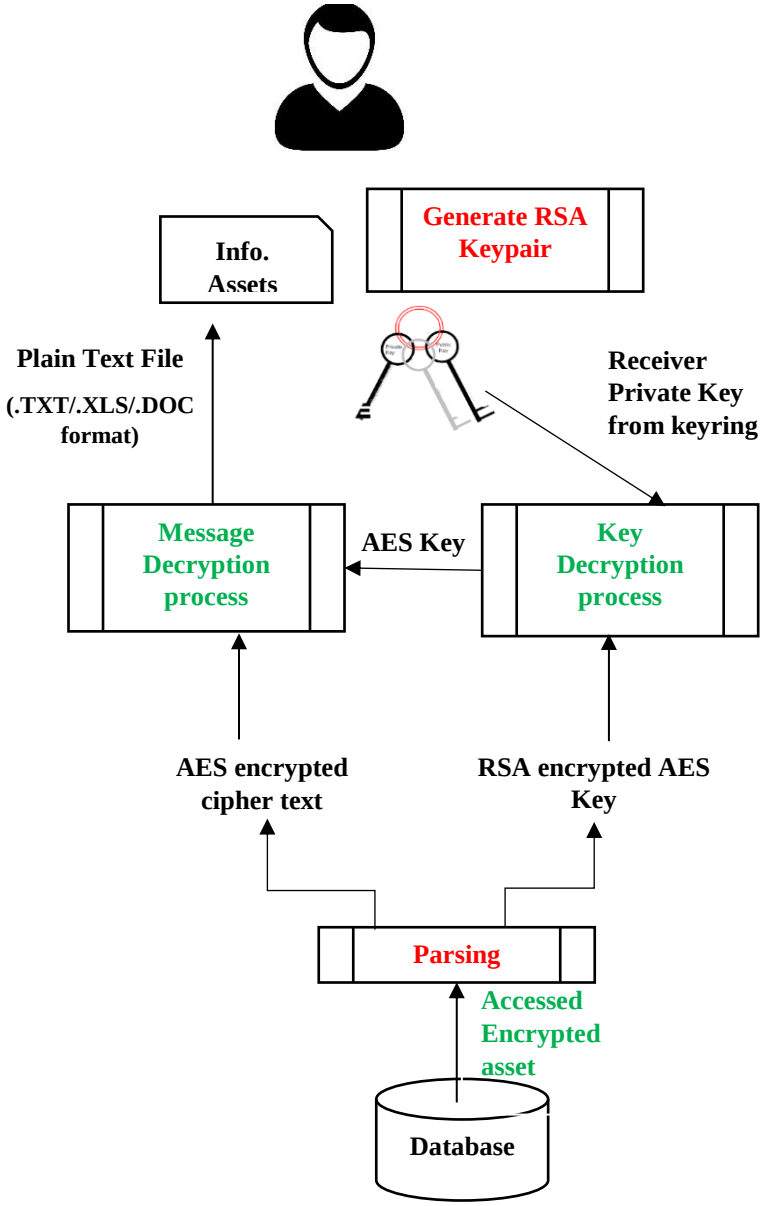



Figure 3.8: Hybrid Decryption using AES & RSA

### 3.6 Summary

This chapter includes all the material used as well as methods developed to propose the solution against URL based phishing attacks. The chapter started with understating the structure of URLs and datasets collected from the UCI machine learning repository. Subsequently, the data processing step is discussed with the feature extract and selection method. Then, model training is discussed with the training and testing dataset. Further model validation and optimization process is presented. Section 2 discussed the working environment used for implementation of proposed work. In section 3 evaluation metrics have been discussed that are used in chapter 4 for evaluation of algorithms. Lastly proposed approach architecture is presented for the detection as well data protection phase.

# CHAPTER FOUR
# RESULT AND DISCUSSION

## 4.1 Introduction

In this chapter, the results of experiments generated by different machine learning algorithms have been proposed. As discussed in the previous chapter implementation has been carried out using the python programming language. Results are evaluated and discussed in detail here with reference to be used.

## 4.2 Experimental Results on URL based Attack Detection

The detection phase, which includes everything from dataset preprocessing to individual algorithm performance evaluation, has been discussed. The result of feature selection is shown in chapter 3 in table 3.1. The result of attribute selection up to performance evaluation is shown in the following subsection.

### 4.2.1 The result on feature selection

Feature/attribute selection is one of the steps of dataset preprocessing. Depending on the result of the RFE algorithms as discussed in chapter 3 in section 3.1.3, the most important features is selected and then the dataset becomes more precise and lightweight. Originally dataset contained 30 features that are reduced into 15 best features. The result of feature selection is shown in following figure 4.1.

```
Num Features: 15
Selected Features: [ True False False False False  True  True  True  True False False False
  True  True  True  True False False False False False False False  True
  True  True  True  True  True False]

Feature Ranking: [ 1  3  9  7 13  1  1  1  1 10 14  4  1  1  1  1  2 11  8 12 16  5 15  1
  1  1  1  1  1  6]



Selected Features: %s
 ['having_IP_Address' 'Prefix_Suffix' 'having_Sub_Domain' 'SSLfinal_State'
 'Domain_registeration_length' 'Request_URL' 'URL_of_Anchor'
 'Links_in_tags' 'SFH' 'age_of_domain' 'DNSRecord' 'web_traffic'
 'Page_Rank' 'Google_Index' 'Links_pointing_to_page']
```

Figure 4.1: List of selected features as output of RFE method

### 4.2.2 The result on Individual Algorithm

An experimental performance evaluation of an individual algorithm is done on the dataset before and after feature selection. That is shown as follows:

**[a] Results before Feature Selection**

In this scenario, all 30 features have been considered and the complete dataset is executed over four selected machine learning classifier/algorithms. Results of the individual algorithm are shown as follows:

1. **The random forest evaluation result**

Table 4.1: Confusion Matrix of Random Forest

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1168 | 42 | 1210 |
| **Malicious** | 44 | 1510 | 1554 |
| **Total** | **1212** | **1552** | **2764** |

TP = 1168 FN = 42 FP = 44 TN = 1510

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1168 + 1510}{1210 + 1554} \quad Accuracy = \frac{2678}{2764}$$

**Accuracy = 96.89%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1168}{1168 + 44} \quad Precision = \frac{1168}{1212}$$

**Precision = 96.36%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{44 + 42}{1210 + 1554} \quad Error\ Rate = \frac{86}{2764}$$

**Error Rate = 0.03110**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1168}{1210}$$

**Sensitivity = 96.52%**

## 2. Decision Tree evaluation result

Table 4.2: Confusion Matrix of Decision Tree

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1205 | 58 | 1263 |
| **Malicious** | 53 | 1448 | 1501 |
| **Total** | **1258** | **1506** | **2764** |

TP = 1205 FN = 58 FP = 53 TN = 1448

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1205 + 1448}{1263 + 1501} \quad Accuracy = \frac{2653}{2764}$$

**Accuracy = 95.98%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1205}{1205 + 53} \quad Precision = \frac{1205}{1258}$$

**Precision = 95.78%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{53 + 58}{1263 + 1501} \quad Error\ Rate = \frac{111}{2764}$$

**Error Rate = 0.0401**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1205}{1263}$$

**Sensitivity = 96.40%**

### 3. Logistic Regression evaluation result

Table 4.3: Confusion Matrix of Logistic Regression

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1070 | 130 | 1200 |
| **Malicious** | 73 | 1491 | 1564 |
| **Total** | **1143** | **1621** | **2764** |

TP = 1070 FN = 130 FP = 73 TN = 1491

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1070 + 1491}{1200 + 1564} \quad Accuracy = \frac{2561}{2764}$$

**Accuracy = 92.66%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1070}{1070 + 73} \quad Precision = \frac{1070}{1143}$$

**Precision = 93.61%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{73 + 130}{1200 + 1564} \quad Error\ Rate = \frac{203}{2764}$$

**Error Rate = 0.0734**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1070}{1200}$$

**Sensitivity = 89.20%**

**4. Naïve Bayes evaluation result**

Table 4.4: Confusion Matrix of Naïve Bayes

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1081 | 142 | 1223 |
| **Malicious** | 125 | 1416 | 1541 |
| **Total** | **1206** | **1558** | **2764** |

TP = 1081 FN = 142 FP = 125 TN = 1416

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1081 + 1416}{1223 + 1541} \quad Accuracy = \frac{2497}{2764}$$

**Accuracy = 90.34%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1081}{1081 + 125} \quad Precision = \frac{1081}{1206}$$

**Precision = 89.63%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{125 + 142}{1223 + 1541} \quad Error\ Rate = \frac{267}{2764}$$

**Error Rate = 0.0965**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1081}{1223}$$

**Sensitivity = 88.40%**

**[b] Results after Feature Selection**

In this scenario, only best 15 features have been considered in dataset that is executed over four selected machine learning classifier/algorithms. Results of individual algorithm are shown as follows:

**1. Random Forest evaluation result**

Table 4.5: Confusion Matrix of Random forest

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1136 | 55 | 1191 |
| **Malicious** | 31 | 1542 | 1542 |
| **Total** | **1167** | **1597** | **2764** |

TP = 1136 FN = 55 FP = 31 TN = 1542

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1136 + 1542}{1191 + 1542} \quad Accuracy = \frac{2678}{2764}$$

**Accuracy = 96.89%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1136}{1136 + 31} \quad Precision = \frac{1136}{1167}$$

**Precision = 97.34%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{31 + 55}{1191 + 1542} \quad Error\ Rate = \frac{86}{2764}$$

**Error Rate = 0.0310**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1136}{1191}$$

**Sensitivity = 95.38%**

**2. Decision Tree evaluation result**

Table 4.6: Confusion Matrix of Decision Tree

| Actual Class | Predicted Class | | Total |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1192 | 62 | 1254 |
| **Malicious** | 62 | 1448 | 1510 |
| **Total** | **1154** | **1510** | **2764** |

TP = 1192 FN = 62 FP = 62 TN = 1510

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1192 + 1510}{1254 + 1510} \quad Accuracy = \frac{2702}{2764}$$

**Accuracy = 95.51%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1192}{1192 + 62} \quad Precision = \frac{1192}{1254}$$

**Precision = 95.05%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{62 + 62}{1254 + 1510} \quad Error\ Rate = \frac{124}{2764}$$

**Error Rate = 0.0448**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1192}{1254}$$

**Sensitivity = 95.05%**

**3. Logistic Regression evaluation result**

Table 4.7: Confusion Matrix of Logistic Regression

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1105 | 129 | 1234 |
| **Malicious** | 82 | 1448 | 1530 |
| **Total** | **1187** | **1577** | **2764** |

TP = 1105 FN = 129 FP = 82 TN = 1448

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1105 + 1448}{1234 + 1530} \quad Accuracy = \frac{2553}{2764}$$

**Accuracy = 92.36%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1105}{1105 + 82} \quad Precision = \frac{1105}{1187}$$

**Precision = 93.09%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{82 + 129}{1234 + 1530} \quad Error\ Rate = \frac{211}{2764}$$

**Error Rate = 0.0764**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1105}{1234}$$

**Sensitivity = 89.54%**

**4. Naïve Bayes feature evaluation result**

Table 4.8: Confusion Matrix of Naïve Bayes

| **Actual Class** | **Predicted Class** | | **Total** |
|---|---|---|---|
| | **BENIGN** | **Malicious** | |
| **BENIGN** | 1092 | 140 | 1232 |
| **Malicious** | 133 | 1399 | 1532 |
| **Total** | **1225** | **1539** | **2764** |

TP = 1092 FN = 140 FP = 133 TN = 1399

$$Accuracy = \frac{TP + TN}{P + N} \quad Accuracy = \frac{1092 + 1399}{1232 + 1532} \quad Accuracy = \frac{2491}{2764}$$

**Accuracy = 90.12%**

$$Precision = \frac{TP}{TP + FP} \quad Precision = \frac{1092}{1092 + 133} \quad Precision = \frac{1092}{1225}$$

**Precision = 89.14%**

$$Error\ Rate = \frac{FP + FN}{P + N} \quad Error\ Rate = \frac{133 + 140}{1232 + 1532} \quad Error\ Rate = \frac{273}{2764}$$

**Error Rate = 0.0987**

$$Sensitivity = \frac{TP}{P} \quad Sensitivity = \frac{1092}{1232}$$

**Sensitivity = 88.63%**

### 4.2.3 Result comparison of Algorithms

In this subsection, the experimental evaluation of the individual algorithm's performance has been compared by means of a table, before and after the feature selection stage of the over test dataset and training dataset.

**[A] Before feature selection over test dataset**

Summary of individual algorithm's result over test dataset before feature selection is shown in table 4.9.

Table 4.9: Result summary before feature selection over test dataset

| Algorithm | Accuracy (%) | Error rate (%) | Sensitivity (%) | Precision (%) |
|---|---|---|---|---|
| RF | 96.89 | 0.0311 | 96.52 | 96.36 |
| DT | 95.98 | 0.0401 | 96.40 | 95.78 |
| LR | 92.66 | 0.0734 | 89.20 | 93.61 |
| NB | 90.34 | 0.0965 | 88.40 | 89.63 |

**[B] After feature selection over test dataset**

Summary of individual algorithm's result over test dataset after feature selection is shown in table 4.9.

Table 4.10: Result summary after feature selection over test dataset

| Algorithm | Accuracy (%) | Error rate (%) | Sensitivity (%) | Precision (%) |
|---|---|---|---|---|
| RF | 96.89 | 0.0312 | 95.38 | 97.34 |
| DT | 95.51 | 0.0448 | 95.05 | 95.05 |
| LR | 92.36 | 0.0764 | 89.54 | 93.09 |
| NB | 90.12 | 0.0965 | 89.01 | 89.14 |

**[C] Before feature selection over Training dataset**

Table 4.11: Result summary before feature selection over training dataset

| Algorithm | Accuracy (%) | Precision (%) |
|---|---|---|
| RF | 99.06 | 97 |
| DT | 99.01 | 96 |
| LR | 93.00 | 93 |
| NB | 90.91 | 90 |

**[D] After feature selection over the training dataset**

Table 4.12: Result summary before feature selection over the training dataset

| Algorithm | Accuracy (%) | Precision (%) |
|---|---|---|
| RF | 98.58 | 97.34 |
| DT | 98.46 | 96 |
| LR | 92.59 | 93 |
| NB | 91.01 | 90 |

### 4.2.4 Performance Comparison with Existing Works

The proposed work is compared with the work of C. Jeeva and E. Rajsingh [69], which is also related to phishing detection with machine learning that claims to have good performance, which uses association rules to detect URLs. Unlike the proposed approach, that work extracted features from URLs and focused on a specific type of malicious URLs. The comparison results are shown in Table 4.13. Although their approach shows good performance, it lacks the analysis and detection of JavaScript code, which is the primary form of attack used in drive-by downloads.

Table 4.13: Result comparison of proposed work with state of the art work

| | **Approach used** | **No. of features** | **Dataset taken** | **Dataset size (Phishing + Legitimate)** | **Accuracy** |
|---|---|---|---|---|---|
| **Jeeva et al.** [69] | Association Rule Mining | 14 | Phishtank | 1400 (1200 + 200) | 93% |
| **Proposed work** | Random forest | 15 | UCI machine | 11055 (6157+4898) | 96.89 |

The above results and comparison clearly shows that the proposed work gives better performance. The reason behind the better result in the proposed work is the size of the dataset. The proposed work used much bigger than the previous study. In this study, Decision tree, Random Forest, Naive Bayes, Logistic regression algorithms are compared over the same dataset to propose the best classifier to detect the phishing attack. Results have shown that random forest gave the best results of accuracy 96.89 over the testing dataset. This is because, random forest collaborates the output of various randomly generated decision trees to produce the final output and it never trusts on the features selected by a single tree. Other than this, it took much more time during training. As compared to a decision tree, which gives rely on a particular set of features generated by single tree. This is the reason, it generated 95.98% accuracy over the testing dataset in the proposed work. The same trends of results are found over training dataset where random forest gave 99.06% detection accuracy as a compared decision tree that gave 99.01% detection accuracy. While, the Logistic Regression classifier algorithm obtained a result of 92.66% over the testing dataset and 93% over training dataset. Naïve Bayes classifier algorithm obtained the lowest result as of 90.34% and 90.91% over testing and training dataset respectively.

To achieve a higher detection accuracy, the classifier must regularly be monitored and updated because phishing techniques vary frequently and use innovative behaviors, conducts, and techniques whenever they active.

### 4.2.5 Experimental Results of data protection model

Data protection is the second phase of proposed research that is dedicated for the protection of informational assets against a phishing attack. To achieve this, the proposed work used a hybrid encryption technique that combined AES and RSA. The proposed hybrid encryption gave strengthening to the data security policies of an organization. In other words, adding to the RSA algorithm with AES provide much more improvement in the security of informational assets. This provides a better security mechanism to protect the organizational assets from security attacks generated by phishers as compared to the individual encryption algorithms. These attacks are analyzed further in the next sub-section. The proposed hybrid algorithm is also implemented in Python with the symmetric key of AES with 128 bits size and asymmetric key of RSA with 1024 bits size. Further, the researcher executed this hybrid algorithm over files of different size and type and observed the result. This hybrid algorithm accepts the files of every type including .doc, .pdf, .xls, .csv etc. that are mostly maintained by any organization. It is observed from the results that encryption time is increased with the increase of file size somehow proportionally, but decryption time takes very less time. Following table 4.14 shows the encryption/decryption time with different files of different sizes.

Table 4.14: Result comparison of proposed work with state of the art work

| File name | Size | Encryption time | Decryption time |
|---|---|---|---|
| Report 2013.docx | 32 KB | 20 ms | 13 ms |
| Sample.docx | 49 KB | 23ms | 14 ms |
| Sample data.csv | 144 KB | 26 ms | 15 ms |
| Afini.xlsx | 850 KB | 83 ms | 24 ms |
| Clinic management.pdf | 1.70 MB | 184 ms | 149 ms |

In general, it is concluded that because of the hybrid algorithm, researchers get:

1. High security level.
2. Assurance of confidentiality of data,
3. Secure transmission of data between entities.
4. Secure data in storage.

### 4.2.6 Security Analysis

The security analysis of the proposed work against security attacks is as follows:

**[A] Man-in-the-Middle attack**

If Phisher wants to do MiTM attack after getting the victim's identity anyhow, and decrypt the message after applying brute force technique to get the symmetric key. They will start communication by observing a session opening on a network. Once a communication session is established between two entities, the phisher can attack the client computer or database to immobilize it, and use IP spoofing to claim to be the legitimate entity and begin operating the session. This attack will be prevented here since the victim does not send the message containing a private key. Since the proposed technique uses hybrid encryption and private is also needed in the decryption process. So, the phisher cannot get the asset since he does not have the private key of the receiver/database.

**[B] Security against Chosen Cipher Text Attacks**

Phisher uses the trick over victims who knows the secret key and send some encrypted message to victim and ask them over the phone call or other that did you get the plain text or not. This process is repeated many times by the phisher. If one of the times, he gets the correct result, he will get the secret key. But in the proposed work, the phisher will never get the secret key, since the key is randomly generated in this system. So even one time a phisher get successful, he will never get the symmetric key, generated for a new message that he/she received. Proposed system protected against such attack.

**[C] Confidentiality**

Since proposed protection model is based on hybrid encryption in which symmetric and asymmetric encryption is incorporated so that it become difficult for adversary to recover any information from cipher text. Since it requires two keys to decrypt the message one is symmetric key that is already encrypted inside message and other is private key, which is only used by the receiver. Thus, proposed data protection model provides data confidentiality.

**[D] Key-recovery attack**

This is an attack that attempt to recover the cryptographic key of an encryption scheme. Since, proposed work have used a random key that changes in every time when new message is encrypted. Thus, it is difficult for the phisher to recover the keys.

## 4.5 Overall Findings

Proposed work is fulfilled all the objectives and solved the both the research questions discussed in chapter 1. The first research question was "*What are the various techniques are available to detect phishing attacks specially URL based and data protect techniques to protect on the organization and individual as on now?*" To answer this question, researcher did lot of survey using literature survey as well as explored lot of research articles to get existing knowledge about phishing detection and data protection. For phishing detection, researcher focused on URL based phishing detection and found research article. Some of them are included in chapter two in section 2.8.1. In these articles most of the researcher used available machine learning algorithm, but very few papers used Random forest algorithm. Similarly, some researchers used ANN method or Software defined platform to detect the phishing attack. This research also found the various datasets for phishing attack like UCI machine learning dataset, Phishtank, Openphish and phishstate. Similarly for data protection this research found available techniques like Anti-phishing software's and tools like eBay and spoof guard and other traditional security protocol like list-based protocols and two-factor authentication system. Other than this most of researcher focused on training of individual. So, all these techniques as of now has been explored for phishing detection and protection in this study.

The second research question was "*How can phishing attack be detected efficiently and organization assets be protected against social engineering attacks?*" To answer this question, this study proposed URL based phishing detection and protection model to detect as well as protect organizational/individual assets from phishing attack.

To detect the phishing attack, this study compared various ML algorithms and found that Random forest gave best results with training as well as testing dataset, that are 99.06 and 96.9 respectively. While worst results are produced by Naïve bias algorithm that are 90.34 and 90.91% over testing and training dataset respectively. This work is also compared with one of

the existing research works [69] and conclude that proposed system is better detect the URL based phishing attack than that work.

As far as protection is concerned, this study proposed data protection model that not only focused on individual's training but also proposed hybrid encryption algorithm to protect the asset that is in transit as well as in storage. Even though, sometime is needed to process the data in encryption and decryption process, but it in millisecond, so it can be affordable. At the same time provide better security to information asset and ensures confidentiality.

## 4.6 Summary

This chapter included various results obtained from experiment of different machine learning algorithms and hybrid encryption algorithm. Further results have been discussed with testing and training dataset as well as after & before feature selection with all machine learning. All results have been evaluated with confusion metrics and further calculated its accuracy, precision and sensitivity with error rate. All results have been organized in the form of tables. Further, proposed detection approach has been compared with existing state of art work. Chapter also discussed results obtained from encryption algorithm by means of encryption/decryption time. Further security analysis is proposed in chapter. At last overall finding has been included in the chapter.

# CHAPTER FIVE
# CONCLUSION AND FUTURE WORK

## 5.1 Conclusion

This study proposed an efficient detection and data protection model against URL based phishing attack. For detection, researcher used ML algorithm like Decision tree, Random Forest, Naive Bayes, Logistic regression algorithms as classifiers to detect the phishing attack. For data protection, researcher used hybrid encryption algorithm to protect the information assets belong to individual/organization.

This study fulfilled all the research objectives by exploring related articles & literature reviews and by proposing the detection and protection model. Further this work answered both the research questions.

In this study, Decision tree, Random Forest, Naive Bayes, Logistic regression algorithms are compared over the same dataset to propose best classifier to detect the phishing attack. Results shown that random forest gave the best results of accuracy 96.89 over testing dataset while decision tree gave the accuracy of 95.98%. Similarly, Logistic Regression classifier algorithm classifies attacks with 92.66% and Naïve Bayes classifies with 90.34 accuracy over testing dataset. In addition, the classifiers are run on the training data, and the same results are obtained. This study found 99.06% detection accuracy in random forest as compared decision tree that gave 99.01% detection accuracy over training dataset.

The data protection model ensures the confidentiality using proposed hybrid encryption. This hybrid encryption used AES and RSA algorithm to encrypt the informational assets. This method ensures protection against various kind of security and crypt-analysis attacks including MiTM, chosen cipher text, key recovery attack etc. The encryption/decryption process take the time in millisecond that is affordable for the user to secure the data. Overall contribution of this thesis includes:

1 Selection of best sets of URL's features and classification algorithm for phishing detection.

2 Experimental evaluation of the performance of the classification algorithms for phishing detection techniques.

3 Ensuring confidentiality to protect information assets using hybrid cryptography.

## 5.2 Future work

Every research has a space to improve, so that proposed work can be extended enough. This study proposes following recommendations for future work:

(1) The proposed detection model can be implemented via a software define network to regularly monitoring and updating the classifier with respect to new phishing attack.
(2) This work does not ensure integrity to information assets that is in transmission. So, some improvement can be possible over proposed data protection model.
(3) Mutual authentication can also be area to be included in proposed work, so that more security can be ensured.

## REFERENCES


[1] M. Aruldoss, N. Anutthamaa, M. Sathyavathy, M. Francois, and V. Venkatesan, "A Framework for Predicting Phishing Websites Using Neural Networks," *IJCSI International Journal of Computer Science Issues*, vol. 8, Sep. 2011.

[2] Namasivayam, "Categorization of phishing detection features," *repository.asu.edu*, 2017.

[3] R. Kalniņš, J. Puriņš, and G. Alksnis, "Security Evaluation of Wireless Network Access Points," *Applied Computer Systems*, vol. 21, Jan. 2017, doi: 10.1515/acss-2017-0005.

[4] N. N. Pokrovskaia and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital' development," in *2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS)*, Sep. 2017, pp. 16–18. doi: 10.1109/ITMQIS.2017.8085750.

[5] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, vol. 59, pp. 186–209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[6] P. L. Gallegos-Segovia, J. F. Bravo-Torres, V. M. Larios-Rosillo, P. E. Vintimilla-Tapia, I. F. Yuquilima-Albarado, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," in *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, 2017, pp. 1–6. doi: 10.1109/CHILECON.2017.8229528.

[7] P. Gallegos, J. Bravo-Torres, V. Larios-Rosillo, P. Vintimilla Tapia, I. Yuquilima, and J. Jara, "Social engineering as an attack vector for ransomware," Oct. 2017, pp. 1–6. doi: 10.1109/CHILECON.2017.8229528.

[8] T. Chuenchujit, "A TAXONOMY OF PHISHING RESEARCH," p. 122, 2016.

[9] "APWG | Phishing Activity Trends Reports." https://apwg.org/trendsreports/ (accessed May 01, 2021).

[10] M. Volkamer, K. Renaud, B. Berens, and A. Kunz, "User experiences of TORPEDO: TOoltip-powered phishing email DetectiOn," *Computers & Security*, Feb. 2017, doi: 10.1016/j.cose.2017.02.004.

[11] Dr. A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "20- A Survey of Phishing Email Filtering Techniques2." Sep. 19, 2015.

[12] "The Man Who Invented Email | TIME.com." https://techland.time.com/2011/11/15/the-man-who-invented-email/ (accessed May 01, 2021).

[13] R. Long, "USING PHISHING TO TEST SOCIAL ENGINEERING AWARENESS OF FINANCIAL EMPLOYEES," 2013. doi: 10.13140/RG.2.1.3846.0565.

[14] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, Oct. 2015, doi: 10.1016/j.ijhcs.2015.05.005.

[15] Dr. A. Almomani, B. B. Gupta, T.-C. Wan, A. Taha, and S. Manickam, "Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection Zero-day Phishing Email," *Indian Journal of Science and Technology*, vol. 6, Feb. 2013, doi: 10.17485/ijst/2013/v6i1.18.

[16] N. An, W. Zhao, J. Wang, D. Shang, and E. Zhao, "Using multi-output feedforward neural network with empirical mode decomposition based signal filtering for electricity demand forecasting," *Energy*, vol. 49, pp. 279–288, Jan. 2013, doi: 10.1016/j.energy.2012.10.035.

[17] C. F. Mohd Foozy, R. Ahmad, and M. Abdollah, “A Practical Rule Based Technique by Splitting SMS Phishing from SMS Spam for Better Accuracy in Mobile Device,” *International Review on Computers and Software (IRECOS)*, vol. 9, p. 1776, Oct. 2014, doi: 10.15866/irecos.v9i10.3909.

[18] S. Heikkinen, “Social engineering in the world of emerging communication technologies,” *Proceedings of Wireless World Research Forum, Serving and managing users in a heterogeneous environment, 17th WWRF Meeting, November 15-17, 2006, Heidelberg, Germany*, p. 10 p, 2006.

[19] H. Nguyen and D. Nguyen, “Machine Learning Based Phishing Web Sites Detection,” 2016, pp. 123–131. doi: 10.1007/978-3-319-27247-4_11.

[20] L. OpenDNS, “PhishTank | Join the fight against phishing,” 2016. https://www.phishtank.com/ (accessed May 01, 2021).

[21] https://apwg.org/trendsreports/ (Accessed May 01, 2021).

[22] E. Lastdrager, “Achieving a consensual definition of phishing based on a systematic review of the literature,” *Crime Science*, vol. 3, p. 9, Sep. 2014, doi: 10.1186/s40163-014-0009-y.

[23] V. Ramanathan and H. Wechsler, “PhishGILLNET-phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training,” *EURASIP Journal on Information Security*, vol. 2012, Dec. 2012, doi: 10.1186/1687-417X-2012-1.

[24] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, “An Empirical Analysis of Phishing Blacklists,” Jan. 2009.

[25] Y. Cao, W. Han, and Y. Le, *Anti-phishing based on automated individual white-list*. 2008, p. 60. doi: 10.1145/1456424.1456434.

[26] S. Chhabra, “Thesis: Fighting Spam, Phishing and Email Fraud,” Oct. 11, 2005. http://alumni.cs.ucr.edu/~schhabra/thesis.html (accessed May 01, 2021).

[27] S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, *A comparison of machine learning techniques for phishing detection*, vol. 269. 2007, p. 69. doi: 10.1145/1299015.1299021.

[28] R. Rao, T. Vaishnavi, and A. Pais, “CatchPhish: detection of phishing websites by inspecting URLs,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, Feb. 2020, doi: 10.1007/s12652-019-01311-4.

[29] D. Sarma, S. Hossain, I. Saha, and M. Alam, *Phishing Attacks Detection using Machine Learning Approach*. 2020. doi: 10.1109/ICSSIT48917.2020.9214225.

[30] D. Sahoo, C. Liu, and S. Hoi, “Malicious URL Detection using Machine Learning: A Survey,” Jan. 2017.

[31] S. R. Safavian and D. Landgrebe, “A survey of decision tree classifier methodology,” *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 21, no. 3, pp. 660–674, May 1991, doi: 10.1109/21.97458.

[32] M. Korkmaz, O. Sahingoz, and B. Diri, *Detection of Phishing Websites by Using Machine Learning-Based URL Analysis*. 2020, p. 7. doi: 10.1109/ICCCNT49239.2020.9225561.

[33] R. Mohammad, F. Thabtah, and T. Mccluskey, *An assessment of features related to phishing websites using an automated technique*. 2012, p. 497.

[34] A. Achuthshankar, A. Achuthshankar, A. K P, and S. N M, “Encryption of Reversible Data Hiding for Better Visibility and High Security,” *Procedia Technology*, vol. 25, pp. 216–223, Dec. 2016, doi: 10.1016/j.protcy.2016.08.100.

[35] C. Shashikala and J. Ajay, “Steganography An Art of Hiding Data,” *International Journal on Computer Science and Engineering*, vol. 1, Dec. 2009.

[36] M. Abadi and R. Needham, *Prudent engineering practice for cryptographic protocols*. 1994, p. 136. doi: 10.1109/RISP.1994.296587.

[37] S. Mare and L. Prodan, *Secret data communication system using steganography, AES and RSA*. 2011. doi: 10.1109/SIITME.2011.6102748.

[38] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986. doi: 10.1007/978-3-642-82865-2.

[39] C. Michael, "What is Data Encryption Standard (DES)? - Definition from WhatIs.com," *SearchSecurity*, May 12, 2017. https://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (accessed May 01, 2021).

[40] G. Singh and S. Kinger, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *International Journal of Computer Applications*, vol. 67, pp. 33–38, Apr. 2013, doi: 10.5120/11507-7224.

[41] F. I. Processing and A. The, *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*.

[42] swenson, "Commerce Department Announces Winner of Global Information Security Competition," *NIST*, Oct. 02, 2000. https://www.nist.gov/news-events/news/2000/10/commerce-department-announces-winner-global-information-security (accessed May 04, 2021).

[43] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[44] N. Hason, A. Dvir, and C. Hajaj, "Robust Malicious Domain Detection," 2020, pp. 45–61. doi: 10.1007/978-3-030-49785-9_4.

[45] S. S. M. Rahman, F. Rafiq, T. Toma, S. Hossain, and K. Biplob, "Performance Assessment of Multiple Machine Learning Classifiers for Detecting the Phishing URLs," 2020, pp. 285–296. doi: 10.1007/978-981-15-1097-7_25.

[46] A. Dan and S. Gupta, "Social Engineering Attack Detection and Data Protection Model (SEADDPM): eHaCON 2018, Kolkata, India," 2019, pp. 15–24. doi: 10.1007/978-981-13-1544-2_2.

[47] A. Jain and B. B. Gupta, "PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning," 2018, pp. 467–474. doi: 10.1007/978-981-10-8536-9_44.

[48] H. Shirazi, B. Bezawada, and I. Ray, *"Kn0w Thy Doma1n Name": Unbiased Phishing Detection Using Domain Name Based Features*. 2018, p. 75. doi: 10.1145/3205977.3205992.

[49] T. Chin, K. Xiong, and C. hu, "PhishLimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking," *IEEE Access*, vol. PP, pp. 1–1, Jun. 2018, doi: 10.1109/ACCESS.2018.2837889.

[50] F. Mouton, L. Leenen, and H. s Venter, *Social engineering attack detection model: SEADMv2*. 2015. doi: 10.1109/CW.2015.52.

[51] A. Van der Merwe, M. Loock, and M. Dabrowski, "Characteristics and responsibilities involved in a Phishing attack," pp. 249–254, Jan. 2005.

[52] T. Thakur and N. Yoshiura, "AntiPhiMBS-Auth: A New Anti-phishing Model to Mitigate Phishing Attacks in Mobile Banking System at Authentication Level," 2021, pp. 365–380. doi: 10.1007/978-3-030-73216-5_25.

[53] S. Hossain, D. Sarma, and R. Chakma, "Machine Learning-Based Phishing Attack Detection," *International Journal of Advanced Computer Science and Applications*, vol. 11, pp. 378–388, Oct. 2020, doi: 10.14569/IJACSA.2020.0110945.

[54] N. Conteh and P. Schmick, “Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks,” *International Journal of Advanced Computer Research*, vol. 6, pp. 31–38, Feb. 2016, doi: 10.19101/IJACR.2016.623006.

[55] A. Singh, V. Kumar, S. Singh Sengar, and M. Wairiya, “Detection and Prevention of Phishing Attack Using Dynamic Watermarking,” 2011, pp. 132–137. doi: 10.1007/978-3-642-20573-6_21.

[56] G. Cj, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha, *PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness*. 2018, p. 181. doi: 10.1145/3270316.3273042.

[57] N. Arachchilage, “Phishing threat avoidance behaviour: An empirical investigation,” *Computers in Human Behavior*, pp. 185–197, Feb. 2016, doi: 10.1016/j.chb.2016.02.065.

[58] A. Diaz, A. Sherman, and A. Joshi, “Phishing in an academic community: A study of user susceptibility and behavior,” *Cryptologia*, vol. 44, pp. 1–15, Aug. 2019, doi: 10.1080/01611194.2019.1623343.

[59] Karakasiliotis, S. Furnell, and M. Papadaki, “Assessing end-user awareness of social engineering and phishing,” *Australian Information Warfare and Security Conference*, Jan. 2006.

[60] R. Kaur, S. Singh, and H. Kumar, “Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches,” *Journal of Network and Computer Applications*, vol. 112, Mar. 2018, doi: 10.1016/j.jnca.2018.03.015.

[61] N. Arachchilage, S. Love, and C. Maple, “Can a Mobile Game Teach Computer Users to Thwart Phishing Attacks?,” *International Journal for Infonomics*, vol. 6, Nov. 2015, doi: 10.20533/iji.1742.4712.2013.0083.

[62] J. S, “Symmetric Key Algorithms: A Comparative Analysis,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, pp. 15772–15775, Sep. 2016.

[63] D. Timothy and A. Santra, *A hybrid cryptography algorithm for cloud computing security*. 2017, p. 5. doi: 10.1109/ICMDCS.2017.8211728.

[64] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, “An Attribute-Based Encryption Scheme to Secure Fog Communications,” *IEEE Access*, vol. 5, pp. 9131–9138, 2017, doi: 10.1109/ACCESS.2017.2705076.

[65] M. Onyesolu and N. Ogwara, “ON INFORMATION SECURITY USING A HYBRID CRYPTOGRAPHIC MODEL,” vol. 4, Nov. 2017, doi: 10.26562/IRJCS.2017.OCCS100080.

[66] S. Rani and H. Kaur, “Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, Art. no. 3, Apr. 2017, doi: 10.26483/ijarcs.v8i3.2990.

[67] V. Kapoor and R. Yadav, “A Hybrid Cryptography Technique for Improving Network Security,” *International Journal of Computer Applications*, vol. 141, pp. 25–30, May 2016, doi: 10.5120/ijca2016909863.

[68] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Phishing websites features,” *School of Computing and Engineering, University of Huddersfield*, 2015.

[69] C. Jeeva and E. Rajsingh, “Intelligent phishing url detection using association rule mining,” *Human-centric Computing and Information Sciences*, vol. 6, Dec. 2016, doi: 10.1186/s13673-016-0064-3.

## APPENDIX

APPENDIX 1: Before feature selection testing dataset result

1. Random Forest

```
Training Accuracy Score Obtained is: 99.06%
Testing Accuracy Score Obtained is: 96.89%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.96      0.97      0.96      1210
Legitimate URL       0.97      0.97      0.97      1554

      accuracy                           0.97      2764
     macro avg       0.97      0.97      0.97      2764
  weighted avg       0.97      0.97      0.97      2764

Confusion Matrix:
 [[1168   42]
 [  44 1510]]
```

2. Decision Tree

```
Training Accuracy Score Obtained is: 99.01%
Testing Accuracy Score Obtained is: 95.98%

Classification Report:
                precision    recall  f1-score   support

 Phishing URL       0.96      0.95      0.96      1263
Legitimate URL       0.96      0.96      0.96      1501

      accuracy                           0.96      2764
     macro avg       0.96      0.96      0.96      2764
  weighted avg       0.96      0.96      0.96      2764

Confusion Matrix:
 [[1205   58]
 [  53 1448]]
```

3. Logistic Regression

```
Training Accuracy Score Obtained is: 93.00%
Testing Accuracy Score Obtained is: 92.66%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.94      0.89      0.91      1200
Legitimate URL       0.92      0.95      0.94      1564

      accuracy                           0.93      2764
     macro avg       0.93      0.92      0.92      2764
  weighted avg       0.93      0.93      0.93      2764

Confusion Matrix:
 [[1070  130]
 [  73 1491]]
```

4. Naïve Bayes

```
Training Accuracy Score Obtained is: 90.91%
Testing Accuracy Score Obtained is: 90.34%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.90      0.88      0.89      1223
Legitimate URL       0.91      0.92      0.91      1541

      accuracy                           0.90      2764
     macro avg       0.90      0.90      0.90      2764
  weighted avg       0.90      0.90      0.90      2764

Confusion Matrix:
 [[1081  142]
 [ 125 1416]]
```

APPENDIX 2: After feature selection testing dataset result

1. Random Forest

```
Num Features: 15
Selected Features: [ True False False False False  True  True  True  True False
False False
  True  True  True  True False False False False False False False  True
  True  True  True  True  True False]

Feature Ranking: [ 1  3  7  6 13  1  1  1  1 10 15  4  1  1  1  1  2 11  9 12 16
  5 14  1
  1  1  1  1  1  8]

 The Accuracy score obtained for training is:  0.985888312628151
Accuracy score obtained for testing is 96.89%
Confusion Matrix:
 [[1136   55]
 [  31 1542]]
```

2. Decision Tree

```
Number Of Features: 15

Selected Features:
[False False False False False  True  True  True  True False False False
  True  True  True  True  True False False False False False False  True
  True  True  True  True  True False]

Feature Ranking:
[ 2  3 12  6 14  1  1  1  1 13 16  5  1  1  1  1  1 10 11  9  8  4 15  1
  1  1  1  1  1  7]

Training Accuracy Score Obtained is: 98.46%
Testing Accuracy Score Obtained is: 95.51%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.95      0.95      0.95      1254
Legitimate URL       0.96      0.96      0.96      1510

      accuracy                           0.96      2764
     macro avg       0.95      0.95      0.95      2764
  weighted avg       0.96      0.96      0.96      2764

Confusion Matrix:
 [[1192   62]
 [  62 1448]]
```

3. Logistic Regression

```
Number Of Features: 15

Selected Features:
[ True False  True False False  True  True  True False  True  True False
 False  True  True  True False False  True False False False False False
  True  True False  True  True False]

Feature Ranking:
[ 1 12  1  4 10  1  1  1 15  1  1  3  5  1  1  1  2 14  1  6 16  7  8 13
  1  1 11  1  1  9]

Training Accuracy Score Obtained is: 92.59%
Testing Accuracy Score Obtained is: 92.37%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.93      0.90      0.91      1234
Legitimate URL       0.92      0.95      0.93      1530

      accuracy                           0.92      2764
     macro avg       0.92      0.92      0.92      2764
  weighted avg       0.92      0.92      0.92      2764

Confusion Matrix:
 [[1105  129]
 [  82 1448]]
```

4. Naïve Bayes

```
Training Accuracy Score Obtained is: 91.01%
Testing Accuracy Score Obtained is: 90.12%

Classification Report:
                precision    recall  f1-score   support

  Phishing URL       0.89      0.89      0.89      1232
Legitimate URL       0.91      0.91      0.91      1532

      accuracy                           0.90      2764
     macro avg       0.90      0.90      0.90      2764
  weighted avg       0.90      0.90      0.90      2764

Confusion Matrix:
 [[1092  140]
 [ 133 1399]]
```

APPENDIX 3: Hybrid Cryptographic Model result


xœó¨t*òLqÍs.Š,□ÉôÏ□□0h□Îyâî'Y□Š1P7{t‹`Ð)—dîï¬'/qeÄÎ™y@±\□¥□$8  C4U1
<,÷×‡ÚßÑÁÛÜîÞ;□□\□rð´éj»na…ìMŸž¬w"9□□¨g□
ŠJÎ£9÷ŸM+□=Ã»¡x˜q^qò9ð™g□=%□çLnA)ªÚkj9IEO„¦².ŠähÎÐ2)□°□□□□¦ûÅ§□ŠW□E¤y„`ëÒ
™$býÕ□;3o`Í!B5AX□□ï□Ll ÅÕ>ìÑìÀô&;□Î□-öæ8+Ž‹µ°ùM*ë|□rn*ØP,¥§6□¿«Øn¦7à□Ô¿E¥G
#□R-ßÈ$°□1g□£□›□^ã□□ Çáf…çtí
□□Î{§;5€Ü4]¯□!C-šä8ÔVG¿3X]□ØU™£nôñý³]ÖÚªí□±"'šóâ{Ó—á/¢B.!Üô}  Ôu½D
{^ë□×ß} Þt-úw|O¡ÆØ'x8À6□□"8□ûñÞËEfÁÅSÿ§ £¼□7-<□Øç•ò‰b3÷□`>X□□□|a8□)ý□ôÎ¥-
□©¢"□ÄæñAØý6¶MÏ¥1w ¯ô³Ê□Äå□¾B™®□ù•□}î÷`Ï^¯PÙR>+r□·¬s?ÅW%+*4N°d»¤□14ÆZ□šfù
Ž□v9î|#@¿²-'šö^□-&ók"¢r-  v□v□‡š□□□Xmªª  %ýî¿íGÁJQ□,□□½i□Ø□æ„Ë\Ï-
Ž=ç¾Þ O2³ÄN□□ew5W□"<£+,e¿ö%□°e.-o:à"Û‡□®*úð·%□
l¼"®'yŽ§ëÑ□□w‡7êÄÒÁ×pÔ/x.f•àm°.D$èÎáÕÔÔ´£"□□Øîé«¢□F□ð□ô@¬-
5£Àxï°w•ôh=É¹Õ□.&ÓÚÃv□®òZ{Á·%[„šÆZýRäK•°€ŒÁiÞ2ö(…É8„¡□□fOKÊž£3ô^Ênë□.zTDH
´¢÷w;Uc0£˜p,æ¦Á$`†,·uÀðZ_ðlÊ□ð¾ó.MÞÊVÒ□°pŠ,□"□8M.zÞ®æ□UWÉSú  æ□FeS¢ü,ä-
□□L□□7-!  pØÖXÝQÊ-„1+UT`"¬BN□€wÂ3©®P~˜R□ñ„□UVÇ€þ±!  ½Ûèé,  ¼Üù§Ž0öÃ)
ªµg5iµÿZú, 0µ"€qœkj {˜Uë½2
ÏÅ<õ□E□kBô¯□ú¥õLIY%2□ŸÛdÓû□□>y±¨û|×Þ‡ê□□□;¤IBöP)=□»à□èÝzK?ƒ%ª)—Ó-
?P0Iü°à□*e-
óI¯ûK□êU□ý¯šxÎjíy*Â¤Cíþ*ó>½□ê!eI□€Ä¶ØÊ□±‹Íf=%AÓ·Ûqòómwáñsãˆš□□8□¤Ÿ□ò□žc
□□□YÄ™þ□ñ\ä□È°)¨n6ÆÜü}ó¥‹Á®D□±,¶Ûæ*tÊ,uA«□□ßBø_d›"□²>□Ì□eÒü
'ÎdÁ‰ □y□6Hİ'.®□[oMŽg².µ°9  L[^5Y1è□Tzí□ß ªä.ê¹:"ÿÓê·,,}°
^#Ð'X…slÇ¿XÆñ'□□Ñ´ëB]žš¡
rï-D›ÇJÒĂi£3Ï÷êšH¢o4À…<-¢sÇUD™>□®0o~ŽüÂŽësË  C±¾^þ äž—
□□@N':67€ïRDÝ@+Sò3bM1˜'Ï/(□ç\þ□x=¦›□ø¤ŒÝ□"pkµ~=šè%¹,
þŒ5!á8",!·□s¨%¹v□LÄ¹2□<□³j4°,³s<□p□
úô J²7z:ã°¡□□°þ9"L³A□Ø□…@Ýa5'QoÕ—rgÁ□ƒ
£t□Þ€½à¦É†~ŒÓt¨¥□Þ□□ã3*E)¥a□H%ë×Â³□ÇÖ□o½□ XcsÚ□□@^â-Å-"@¨ÇCe □.¥øÍ-
BÐŸ†¹§zjˆU÷ÎTX8V"NÜ|×4-□G□°□çŒ7èbéæ□v□Ê¼Ç1!<R/}Ü3w!‡íÁwÏ®ÇÄ-~ùï□¯œU&
i¦¤T
ÃGGˆ□ü3@2\ßB)□□0‡°Ö-Rˆ¦□□eé¼¶CbM,£³%-¾|-
ƒIZì«žyÚ,%Â\š\=ësvè□´G™)Ä{w□"□\□xò$«FVSO1›¿k^=¥ŸŸ Ky‡□¤½i#□ŒâÎõÚm<û>□s)ˆd
à¾¹□œ}ý¢Šp□ë-kU□¶˜YŒ—§ˆDdÑ"`ãR™Q0Ø□Aˆ[□ð1$1È□hŒ#Á□l□euíÞee8VU|Nž"Ì□Ò:m