1. REQUIREMENT ANALYSIS

3.1 Customer Journey Map

Introduction:

This document presents a Customer Journey Map created as part of the 'Exploring Cyber Security: Understanding Threats and Solutions in the Digital Age' project. The primary goal of this project is to investigate current cybersecurity challenges by identifying and analyzing vulnerabilities within web applications. This map visualizes the typical user's interaction with the cybersecurity aspects of the target website, [Target Website Name]. By understanding the user's journey, we aim to highlight potential security concerns and identify opportunities to enhance both the security and user experience of the website.

User Persona:

The map focuses on the 'Typical Web Application User,' a persona representing a general user interacting with the website. This user has a basic understanding of web browsing but may not possess in-depth cybersecurity knowledge. They expect the website to be secure and trustworthy but may not always be aware of potential risks.

Cybersecurity Context:

Cybersecurity is paramount for protecting users and the website itself from various threats. This map illustrates potential risks users may encounter, such as data breaches due to vulnerabilities like SQL Injection, Cross-Site Scripting (XSS), and Authentication Bypass. The project involves using industry-standard scanning tools like Nessus, Burp Suite, and OWASP ZAP to identify these weaknesses and recommend remediation measures. Understanding the user's journey in relation to these vulnerabilities is crucial for developing effective security solutions and improving user confidence.

Map Overview:

The map outlines the user's journey across key stages, including Initial Exposure, Authentication, Data Input, Error Handling, and Post-Interaction. For each stage, it details typical user actions, thoughts, feelings, and the relevant cybersecurity considerations. This visualization will help in prioritizing security enhancements and ensuring a more secure and user-friendly experience.

Customer Journey and Cyber Threats

87%
of shoppers say social media helps them make a shopping decision[2]

25%
of business sell trough Facebook

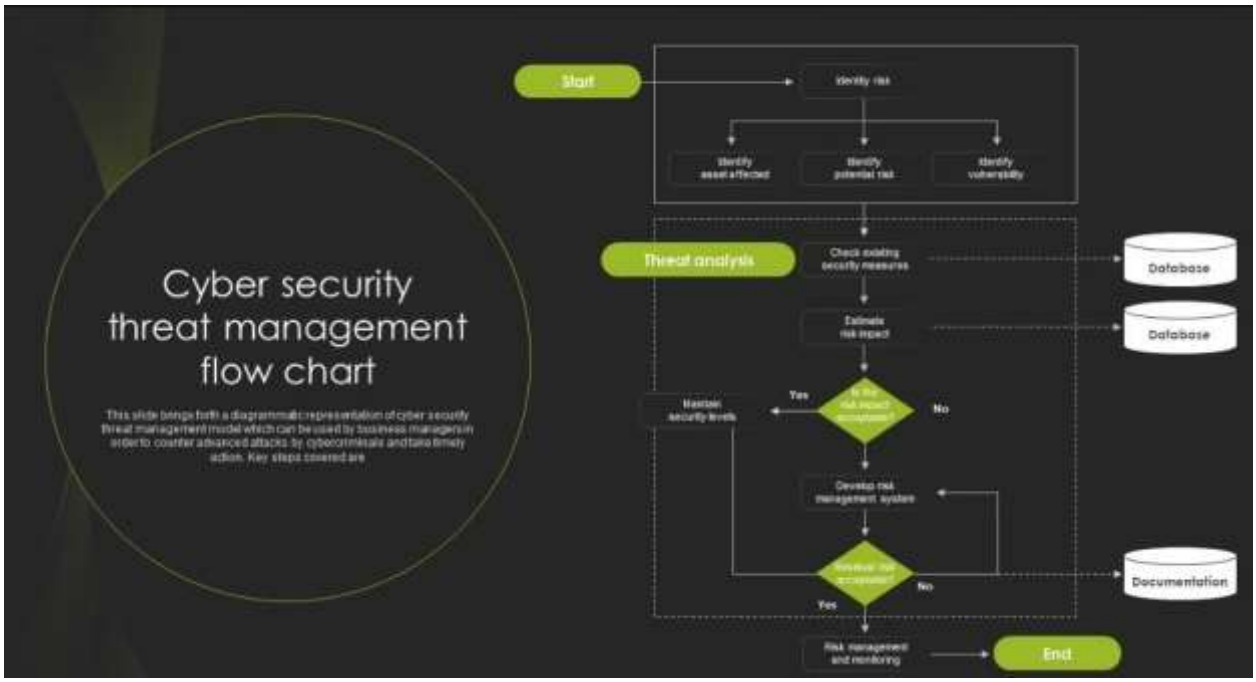
1. DBIR, Dec. 2018
2. Absolunet, ecommerce trends 2019

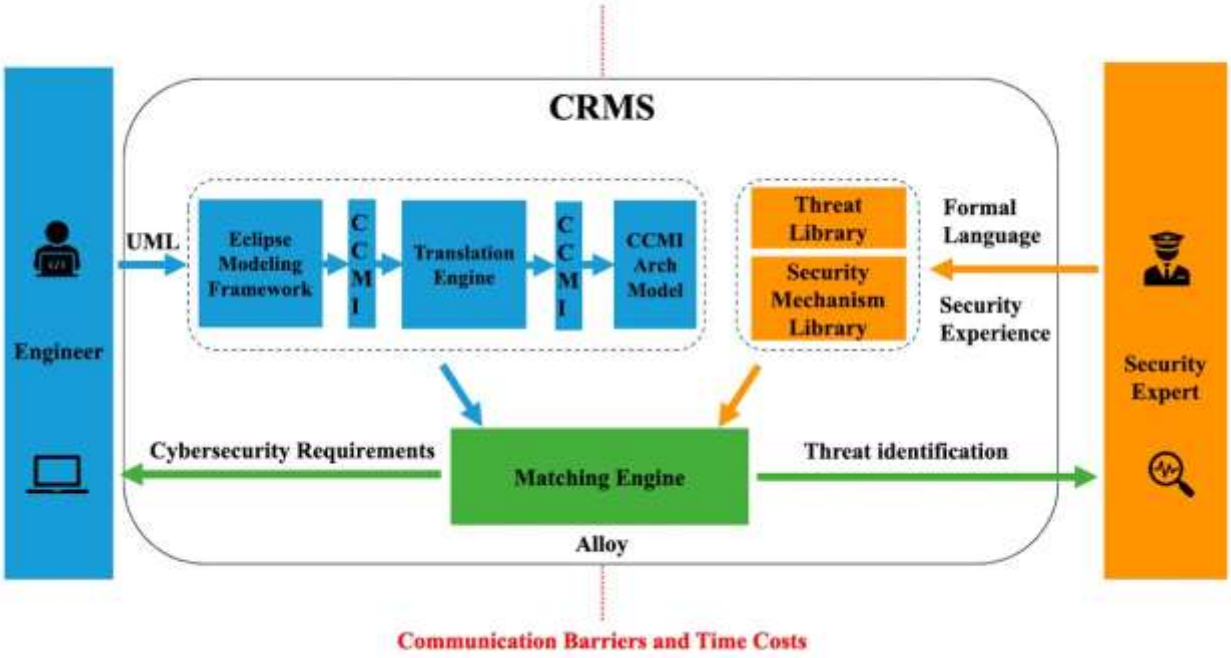
3.2 Solution Requirement

To develop an efficient phishing detection system, the following components are required:

- **Data Preprocessing Pipeline** – Cleans and structures the email data for analysis.
- **Machine Learning Model** – A classifier trained on phishing and legitimate email datasets.
- **Performance Evaluation Framework** – Assesses accuracy, precision, recall, and F1-score.
- **User Notification System** – Alerts users about detected phishing emails.
- **Deployment Infrastructure** – A web-based or API-driven system for real-time email classification.

3.3 Data Flow Diagram




CRMS
Engineer
UML
Eclipse Modeling Framework
CCMI
Translation Engine
CCMI
CCMI Arch Model
Threat Library
Security Mechanism Library
Formal Language
Security Experience
Security Expert
Cybersecurity Requirements
Matching Engine
Threat identification
Alloy
Communication Barriers and Time Costs