CTICTR
CURRENT TRENDS IN INFORMATION COMMUNICATION TECHNOLOGY RESEARCH

BABCOCK UNIVERSITY
KNOWLEDGE TRUTH SERVICE
ILISHAN - REMO, NIGERIA.

CTICTR 4(1): 61 - 78 (June 2025)

ISSN: 2814-1709

Received: 06-03-2025

Accepted: 02-06-2025

**https://doi.org/10.61867/pcub.v4i1a.199**

# DEVELOPMENT OF A SECURE LOAN APPLICATION USING SCAM BAITING FRAMEWORK FOR DETECTING BAD ACTORS

**Opeyemi Joshua Adelowo**

**Oluwabukola Funmilola Ajayi**

**Alfred Udosen**

Corresponding Author Email: adelowoop@babcock.edu.ng

School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

# Development of a Secure Loan Application using Scam baiting Framework for Detecting Bad Actors

Opeyemi Joshua Adelowo [1*], Oluwabukola Funmilola Ajayi [2], Alfred Udosen [3],

[1]*Department of Information Technology, Babcock University, Ilisan-remo, Ogun State*
[2,3]*Department of Computer Science, Babcock University, Ilisan-remo, Ogun State*

Email: adelowoop@babcock.edu.ng[1], ajayioluwa@babcock.edu.ng[2], *udosena@babcock.edu.ng* [3]

***Abstract***

Loan applications have become popular for managing loans through mobile devices, offering convenience and personalized loan offers. However, there are concerns about bad actors who borrow without paying back. Scam baiting, a technique for overcoming these difficulties, entails luring users into participating in activities that reveal their illegal activities and then, turning them over to the authority. In this paper, the goal was to create a secure Progressive Web Application (PWA) mobile application that uses scam baiting methods to discover bad actors. This study focuses on creating a secure loan application using a framework that identifies and exposes loan defaulters. Agile extended programming, which allowed for flexibility and adaptability during the development process, was the methodology used in this study. The researcher used the magnetic honeypot technique, which entails constructing a target that is alluring to them. Zero loan credit rate and lack of a credit history was used in this regard. The Loan Bureau API was used to confirm the user's status, while the Youverify API was used to ensure the authenticity of the user. Ten people were chosen at random to take part in the loan application Test. 7 of the participants were discovered by the system to have previously borrowed from other loan applications, while 3 individuals were confirmed as trustworthy borrowers with no prior history of fraudulent loan activity. This distinction confirmed the framework's accuracy in separating legitimate borrowers from prospective con artists. This outcome illustrated the scam-baiting framework's effectiveness in locating persistent loan defaulters.

***Keywords:*** *Scam baiting, Framework, Loan Application, Bad Actors*

**Word count:** 249

## 1.0 Introduction

A growing number of cyberattacks on different computer systems (Personal Computers, Servers, Mobile Devices, Internet of Things, Cloud Computing, and so on) over the last decade have made cybersecurity a significant issue in both the public and private sectors. A greater understanding of the dangers and vulnerabilities related to digital environments has arisen as a result of this growing threat. Currently, it's not worth it to invest in a system that wasn't designed with safety in mind. The constant presence of anonymous "bad guys" and "hackers" who prowl the Internet in search of vulnerabilities has elevated the importance of addressing cybersecurity concerns. An enormous amount of attention has been paid in recent years to comprehending the complex cybersecurity landscape. As a result, a new branch of study called "cyber criminology" has emerged. Researchers in this field explore into the underlying problems that fuel illegal activity and other types of wrongdoing online. They also look at the moral and legal implications of these problems, as well as the solutions developed to deal with them. Inquiries on the creation, enforcement, and breach of laws are crucial to this field of research, especially when taking into account how empirical studies affect police and criminal justice practises. [1]. However, Scam baiting is a novel cybersecurity strategy that entails luring fraudsters onto various networks in order to expose and publicise their nefarious actions [2].

Researchers have discovered that Scam baiting might be a fun way to educate people about the risks of scamming. Scam baiters inform the public about these fraudulent practises by demonstrating different scams and how they operate on social media sites like YouTube. Scam baiting videos' attractive appeal serves two purposes. First of all, it grabs people's attention and alerts them to the dangers of scams. Second, it makes the fraudulent actions visible to a large audience, making con artists feel accountable. Unexpectedly, the proliferation of online video material is to blame for the rising popularity of social media sites, especially YouTube. These sites encourage users to view and follow interesting videos, including Scam baiting ones. This increase in viewers suggests a growing interest in these videos, which broadens the audience for the impact of Scam baiting campaigns. As a result, Scam baiting has been successful in achieving its goals of educating audiences about scammers' tactics while also entertaining audiences. This has helped to raise public awareness of and comprehension of online scams [3]. The film, titled "This is what happens when you react to a spam email," was published online by TED on January 8, 2020. The

video gained millions of views and comments in only a few days after it was released. It would be difficult to describe what a scam bait is without first defining a scam. Several books and articles have written about various forms of scams, such as technical assistance scams [4] and advance-fee scams [5], [5]; but, a lot of study also looks at Scam baiting from the point of view of online vigilantism or digitalism [6], [6], [3].

Scam baiting, a practise designed to trick and expose people engaging in shady business dealings like the 419 scam, can be driven by a sense of moral obligation. The Nigerian-originated 419 swindle has gained a lot of attention [7]. This specific con has drawn a lot of attention and been the topic of in-depth investigation and discussion.

Mobile applications known as loan apps let consumers apply for and manage loans online using their cell phones or other mobile devices. The amount of customers utilising mobile apps to manage loans has dramatically increased in recent years, according to a 2020 study from the Consumer Financial Protection Bureau (CFPB) [8]. Loan applications offer borrowers more convenient access to loans, which is one of its advantages. Borrowers can monitor their accounts and submit loan applications via loan apps at any time, from any location. Borrowers who need to apply for loans fast or who have restricted access to regular banking facilities may find this to be of great benefit.

The fact that loan applications frequently employ cutting-edge technology, like artificial intelligence (AI) and machine learning, to deliver more individualized loan offers and quicker approval timeframes is an additional advantage. Loan applications can provide borrowers loan offers that are suited to their specific needs by using data such as credit history, income, and spending patterns to analyse.

But loan applications could potentially come with hazards. One worry is that some users may be tempted to incur more debt than they can handle due to the convenience and simplicity of these apps. In addition, some lending applications could charge consumers with exorbitant interest rates or hidden costs that are not adequately disclosed.

Loan-related fraud was the second most prevalent type of fraud reported to the Federal Trade Commission (FTC), accounting for 9% of all fraud claims, according to a 2020 report by the agency

[9]. The most frequent types of loan-related fraud reported to the FTC were imposter schemes, followed by identity theft and application fraud.

Borrowing activity has increased significantly in recent years as a result of the growth of phone applications that offer quick and convenient loan services. The high percentage of borrowers who default on their loans, which causes financial losses for lenders and could have a negative impact on the lending ecosystem, is a significant cause for concern.

Some research have examined scam characteristics from a Scam baiting perspective, but there hasn't been much effort put into developing a comprehensive Scam baiting framework for loan web application.

The researcher leveraged the findings from the development of a secure loan application using Scam baiting framework that can detect bad actors on loan application using a Progressive Web Application (PWA). The specific objectives are to develop a Scam baiting framework that attracts persistent loan defaulters.

## 2.0 Literature Review

What is security?

Security is the condition of being free from risk, harm, or loss. The protection of digital assets, such as data, systems, and networks, from illegal access, use, disclosure, interruption, alteration, or destruction is referred to as security in the context of information technology [10].

Security is a broad notion that includes a number of aspects, such as authenticity, non-repudiation, availability, and secrecy. Although integrity refers to the guarantee that data has not been tampered with or altered, confidentiality refers to the safeguarding of sensitive information from unauthorised disclosure. While authenticity refers to the guarantee of the identity of the user or system, availability refers to users' capacity to access and use digital assets when necessary. The capacity to demonstrate that a user or system has carried out a specific activity is known as non-repudiation [10].

Modern civilization places a high priority on security, which includes a wide variety of issues from national security to personal safety. Security is now much more necessary as the world becomes increasingly globally interconnected. Using recent research and articles as a foundation, this response will investigate the notion of security in general.

### *2.1 Overview of Scam*

Scams are deceptive practises when an individual is deceived into parting with money or private information. Swindlers are resourceful people who consistently devise novel methods of defrauding others. Customers may be contacted in a variety of ways, including over the phone, in the mail, by email, or even in person at their homes. In the lengthy history of frauds, the internet is a relatively new avenue for con artists to discover prospective victims. However, they have quickly adapted traditional methods to the emerging digital landscape according to the latest available data [11].

## 3.0 Methodology

### 3.1 In developing a secure loan application that attracts persistent loan actors (defaulters):

- The database used for the system was designed using MYSQL database and was implemented with XAMPP database management system.
- The progressive web application was divided into client and server sides. The client side was built using hypertext Markup Language (HTML), Cascading Style Sheets (CSS) and JavaScript. The server side was built using the framework of Hypertext Pre-processor (PHP), Laravel.

For this study, Agile extensible programming was applied. The design and execution of software systems that may be easily expanded or modified to suit future modifications and enhancements is known as extensible programming. It entails developing adaptable, modular, and scalable software structures, frameworks, and components.

For this study, the quasi-experimental research design was used as the technique of inquiry. Although this study employs experimental methodology, it cannot be considered a true experiment since there is no specific hypothesis to be tested and no controls have been included.

This study investigates potential strategies for constructing a "Scam baiting" framework that might be used to counteract fraudulent activity across several Internet venues. To achieve this, the following procedures are given for developing a Scam baiting framework appropriate to the research objective.

One goal is to examine how various Scam baiting models fare against one another. The study's focus is on current Scam baiting practices. By analysing these, we may better understand the ethical implications of the present architecture and design a more suitable replacement.

Second, a 3D model of the structure was created using Concept Draw PRO.
Thirdly, the researcher used the framework described in (2) to design honeypot loan web app that is expected to detect bad actors that desires to borrow or take loan from different loan lenders without paying back.

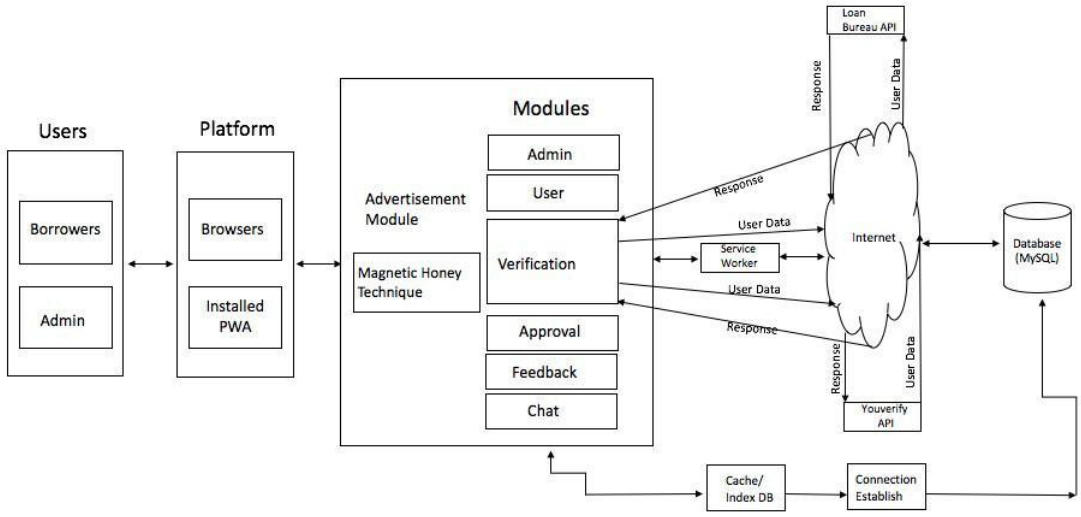



Figure 1: The proposed admin Use Case Diagram

The model in figure 1 constitutes the following key elements:

**Users**: This includes all users accessing the loan application thereby having access to its functionality based on the assigned role. Users can be at any location while accessing the platform

**Platforms**: These are mobile devices of different sizes and form factors used in accessing the application. Users can make use of web browsers on their devices or click on the installed application on their devices after the first visit. Platforms could be android based, iOS-based, windows based, or any other smartphone that has an updated and functional browser.

**Advertisement Module (Magnetic Honeypot Technique):** Just as the common Magnetic honeypot system, the platform uses zero payback rate and no loan credit history to attract users to the system.

**Admin Module**: The admin has the privilege of login, change password, view loan request, flag loan request, view flagged requests, send flagged requests, add admin, delete admin, view admin and logout when all has been done.

**User**: The user has the following privileges; click apply button, fill the KYC, check loan request status and logs back to the system.

**Verification**: The admin verifies each user by comparing the supplied information with the information provided by (youverify), to confirm the correctness of the provided information by the user. More so, there exist response and user data at this stage which is dependent on internet before moving to the next stage. Also, the gathered information is been sent through

the phone Bureau API to see if the user has borrowed from other places, the result at this stage shows if the user is a bad actor or not.

**Approval**: The admin approves the loan result based on the result from the verification module.

**Feedback**: The user gets a feedback on the loan request after all the modules had been completed.

**Loan Bureau Api**: Checks if the user has borrowed consistently from other loan application.

**Youverivy Api**: it verifies the legitimacy of the user through the users' BVN.

**Service Worker (SW)**: By intercepting the users' requests, this is the main element of Progressive Web Application (PWA) technology that enables quick responses to the consumers. The SW implements the cache first response method after intercepting the user's request by looking in the cache for the appropriate response to the user's request. This reduces the need for a database round trip. While transmitting the response to the user, a copy of the response and the accompanying request identity is preserved in the IndexedDB. Only if there is a cache miss is the journey to the cloud functions and database made. In contrast, if the user is off-line, the request (GET and POST) is fetched and sent from/to the IndexedDB; in this case, the users' requests can be captured and registered as a synchronisation task; once this happens, the task must wait until a connection is made to the internet before being pushed to the database through the background thread.

**Network (HTTPS)**: This represents requests sent to the internet through the Hypertext Transfer Protocol Secure (HTTPS). Service workers work only with the HTTPS protocol, this is so to enable the integrity and confidentiality of data transmitted.

**IndexedDB:** This object-oriented transactional database system for JavaScript offers a low-level API for client-side storage of substantial amounts of structured data (including files). With the use of indexed keys, it performs fast searching of data items. In order to avoid blocking other application operations, operations (create,

read, update, and delete) conducted using the IndexedDB are carried out asynchronously.

**Database (MySQL)**: All of the loan application's data are saved as documents and arranged into collections in this NoSQL (document-oriented) database. It makes data synchronisation and querying easier with the programme.

**Chat Module**: Here, the administrator engages with the user to further establish the user's legitimacy.

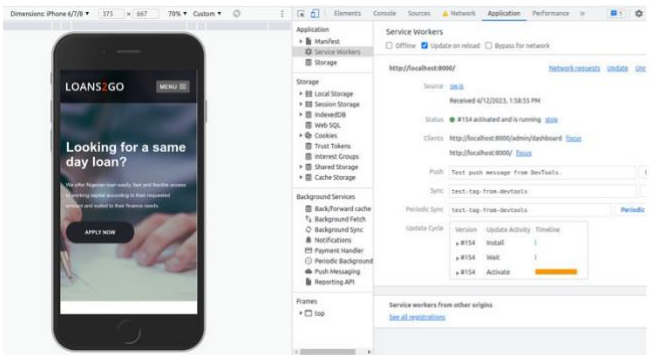
## 4.0 Implementation of Loan application

### 4.1 Application Shell

The application shell contains a minimal HIML, CSS, and is needed to power the user interface of the LOANS2GO in the first render of the application; the essence of this is to present immediate Intents to the user irrespective of the network status. The app shell for the LOANS2GO app makes use two (2) versioned caches to store static and dynamic contents respectively.

### 4.2 Service Worker Integration

Service workers have a significant role in the operations of the LOANS2GO loan application. Service workers help the loan application to defer actions until the user has a stable internet connection.



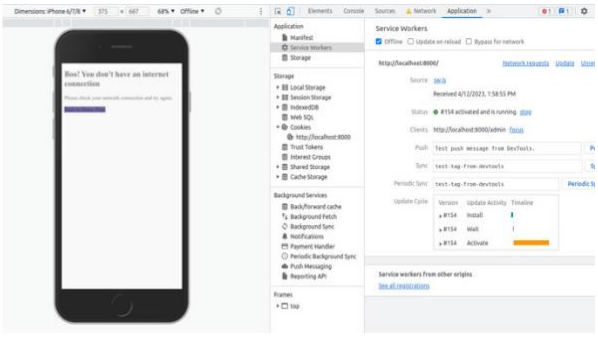



Figure 3: User home page in an offline state

Figure 2: User home page in an online state

Users can navigate to the apply loan page, check the progress of their loans, and other routine tasks while offline. Figure 2 depicts the user in an online condition, whereas Figure 3 depicts the person in an offline state.

### 4.3 Web Application Manifest (App Manifest)

This is a file that gives a developer a way to turn web pages into mobile applications so they can be installed on users' devices and accessed from their pool of installed apps.

The web manifest for the LOANS2GO has been decrypted from the manifest.json using the developer tools in the Google Chrome browser as shown in the Figure 4

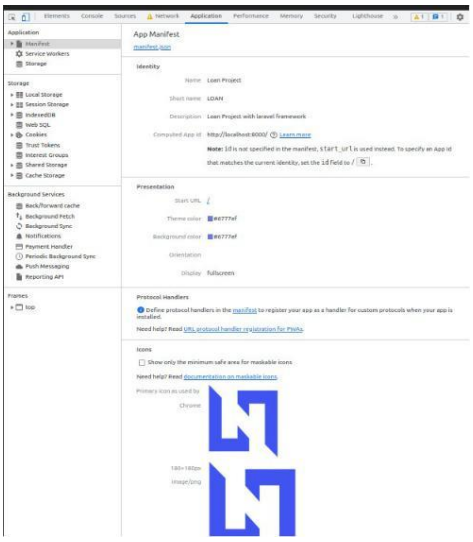



Figure 4: The interpretation of the manifest.json file by Google Chrome Browser

The web page can be packaged as a mobile application, downloaded to the user's device, and accessed from the user's home screen with the aid of the well-documented web app manifest file. The programme icon is added to the user's home application list (or home screen) following a successful installation on the user's device, as seen in Figure 5

Figure 5; LOANS2GO application icon alongside other application icons

From this point forward, the online application is now a mobile application and operates on the user's device as a standard app and has access to all of the capabilities. While online, the application gradually prepares for periods when the network is unstable or there is a complete loss of internet access, allowing users to perform routine tasks like travelling to the loan application page, checking the status of their loans, and so on. The user's home page is depicted in Figure 6.

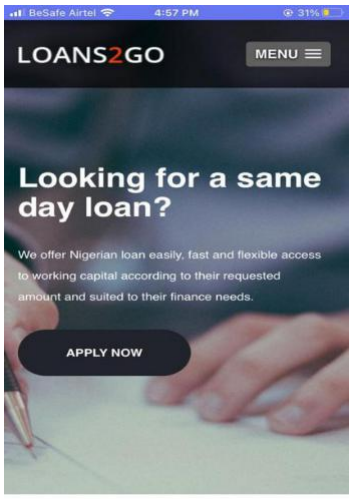



Figure 6: User LOANS2GO Home Page

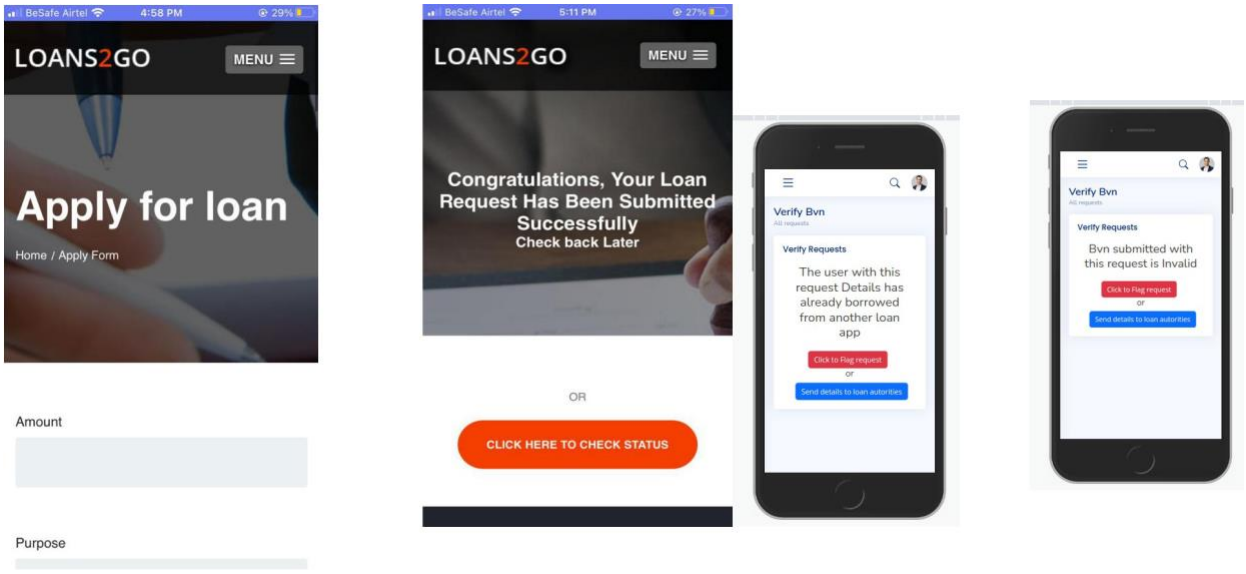



Figure 7: LOANS2GO Loan Form/ Request Successfully Submitted and Figure 8: Invalid BVN page/ Admin page showing user has already borrowed loan from another app

Figure 7 depicts the LOANS2GO Loan Form or Successfully Submitted Request, while Figure 8 displays invalid BVN page or Admin page showing that user has already borrowed loan from another app.

### 4.2a Tested Results

Table 1: Bad actors

| S/n | Name | Amount Requested | Purpose of Loan | Employment Status | BVN |
|---|---|---|---|---|---|
| 1 | SAMPLE 1 | ₦70,000 | To get a new accomondation | Unemployed | ********** |
| 2 | SAMPLE 2 | ₦65,000 | To pay my house rent | Unemployed | ********** |
| 3 | SAMPLE 3 | ₦90,000 | I need this Loan for my school project | Unemployed | ********** |
| 4 | SAMPLE 4 | ₦50,000 | To start new Business | Employed | ********** |
| 5 | SAMPLE 5 | ₦45,000 | For a personal Project | Employed | ********** |
| 6 | SAMPLE 6 | ₦80,000 | In order to pay my son's school fee | Unemployed | ********** |
| 7 | SAMPLE 7 | ₦100,000 | To get a new accomondation | Employed | ********** |

### 4.4.2b Tested Results

**Table 2: Showing Details of Confirmed Request**

| S/n | Name | Amount Requested | Purpose of Loan | Employment Status | BVN |
|---|---|---|---|---|---|
| 1 | SAMPLE 8 | ₦55,000 | To start new Business | Unemployed | ********** |
| 2 | SAMPLE 9 | ₦70,000 | In order to pay my son's school fee | Employed | ********** |
| 3 | SAMPLE 10 | ₦40,000 | For a personal Project | Employed | ********** |

Table 1 of the table depicts seven users who borrowed money from another phone app with their details, whereas, Table 2 depicts three users who are legitimate users.

## 5.0 Summary, Conclusion and Recommendation

The development of a secure loan application using Scam baiting framework for detecting bad actors has proven to be a fruitful method for locating and outing persistent loan defaulters. The precise goal of this study was to develop a secure loan application using Scam baiting framework that would draw in the bad actors. The framework was created and implemented using an agile extreme programming with a focus on those who have a history of loan default. The framework used a variety of baiting strategies (no interest loan rate and no loan history) to entice these bad guys while capturing vital data regarding their actions and intentions.

The information gathered through the framework was subsequently reported to the relevant authorities, aiding in the prevention of additional fraudulent activities and protecting potential victims. The results of this study revealed that 10 users were used, 7 of the participants had borrowed from other sources while 3 were legitimate users and not defaulters.

The findings of this study point to a sizable vacuum in the body of knowledge regarding how scammers exploit loan applications. This discovery emphasises the demand for additional study and research in this field. Recognizing this gap makes it clear that more effort is needed to broaden and improve the body of knowledge in this particular sector.

Future academics should concentrate on performing thorough investigations to look deeper into the prospect of utilising loan applications as a strategy for scamming unscrupulous individuals. Researchers can investigate various strategies, techniques, and frameworks to draw in and reveal persistent loan defaulters by expanding on the basis laid out in this study. Investigating various methodologies, such as agile extensive programming or other cutting-edge strategies, can also help to improve and maximise the efficacy of such frameworks.

## REFERENCES


[1] K. S Choi *The Present and Future of Cybercrime, Cyberterrorism, and Cybersecurity,* International Journal of Cybersecurity Intelligence & Cybercrime, 2018.

[2] L. Samuli, L. & R. Sampsa *Scam baiting as a form of online video entertainment: An exploratory study,* Researchgate, 2021

[3] T. Sorell, *Scam baiting on the spectrum of digilantism*, Criminal Justice Ethics, 153-175. 2019

[4] S. L. Rauti "You have a Potential Hacker's Infection: A Study on Technical Support Scams" ,in *IEEE International Conference on Computer and Information Technology (CIT)*, 2017, pp.197-203.

[5] T. Holt, "Aqualitativeanalysisofadvancefeefraude-mailschemes", *International Journal of Cyber Criminology,* pp. 1-8, 2015

[6] J. W. Smallridge, "The rise of online vigilantism", *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp.1307-1331

[7] T. Sorell, "Scam baiting on the spectrum of digilantism". *Criminal Justice Ethics*, pp.153-175, 2019

[8] Consumer Financial Protection Bureau. (2020). Use of Mobile Financial Services for Borrowing Among Underbanked Consumers. https://files.consumerfinance.gov/f/documents/cfpb_mobile-financial-services-for-borrowing-underbanked-consumers_2020-10.pdf

[9] Federal Trade Commission. (2020). Consumer Sentinel Network Data Book 2020. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_data_book_2020.pdf

[10] Martin, R. C. (2017). Agile Software Development: Principles, Patterns, and Practices. Pearson Education.

[11] W. Ruth (2014, April 15). *Internet Security*.(online) Available http://courses.cs.washington.edu/courses/csep590/06au/ projects /hacking.pdf>