MINI PROJECT – II : SYNOPSIS REPORT

“BIFROST : “More Than a Firewall, A Digital Guardian”

by

Ankit Kumar Singh

22bcs015

Apiksha

22bcs020

Soumitra Rai

22bcs090

Under the Guidance of Dr. Rohit Tanwar

Submitted in partial fulfilment of the requirements for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

SHRI MATA VAISHNO DEVI UNIVERSITY, KATRA

(School of Computer Science & Engineering)

JAMMU & KASHMIR – 182 320

Session 2022-26 (Even)

1. INTRODUCTION

With children's increasing use of digital devices, parents and guardians face challenges in monitoring and controlling in-app purchases and online transactions. Many applications and games feature easy payment options, making it possible for kids to unknowingly or impulsively make purchases without proper authorization. This can lead to unexpected expenses and security risks.

To address this issue, our project introduces a firewall service in the form of a cross-platform desktop application for Linux, Windows, and macOS. This firewall identifies payment gateway links and redirects them to a designated parent or guardian for approval before allowing the transaction to proceed. This ensures that only authorized purchases are completed, providing an additional layer of financial control and security.

For now, the primary focus is on payment approval, but future enhancements will include ad-blocking, malware protection, and additional security features to further safeguard children's online experience. This firewall service aims to empower parents and guardians by giving them greater oversight over digital spending, ensuring a safer and more controlled online environment for their children.

2. RELATED WORK

Parenting in the digital age is tough. While parental control apps help with screen time and content filtering, they often fail to prevent unauthorized payments and protect kids from online threats.

Apps like Google Family Link, Apple Screen Time, and Microsoft Family Safety help manage screen time and filter content, but they lack key protections like blocking unauthorized payments and detecting scams. [2]

These apps mostly restrict access but don't stop unauthorized payments or protect kids from online scams.

Studies highlight children's digital vulnerabilities. Kids often make accidental in-app purchases, as seen in Amazon's lawsuit over unauthorized transactions. They're also highly susceptible to malicious content due to weak ad detection. Scammers target them with fake job offers, posing as TikTok employees to steal money or information. These risks emphasize the urgent need for stronger online protections to safeguard children from financial loss, deception, and fraud. [1]

Despite the availability of parental control applications, significant gaps remain. Existing tools lack real-time transaction approval, preventing parents from authorizing or denying purchases as they occur, which can lead to unauthorized expenditures. Additionally, current solutions fail to provide robust scam and phishing prevention, leaving children exposed to fraudulent ads and phishing websites. Furthermore, many applications rely on static threat detection with

predefined rules rather than adaptive, real-time analysis, making them ineffective at identifying emerging online threats. [3]

3. PROBLEM STATEMENT

With children's increasing use of digital devices, parents and guardians face significant challenges in monitoring and controlling in-app purchases and online transactions. Many applications and games feature easy payment options, allowing children to unknowingly or impulsively make purchases without proper authorization. This can lead to unexpected expenses and security risks for families.

4. OBJECTIVE

The primary objective of this project is to develop a firewall service as a cross-platform desktop application for Linux, Windows, and macOS that helps parents and guardians regulate online transactions made by children on shared devices. The firewall will:

1. Identify payment gateway links in real time before transactions are processed.
2. Redirect payment requests to an authorized parent/guardian for approval.
3. Prevent unauthorized or accidental purchases, ensuring financial security and parental control.
4. Provide a seamless and user-friendly interface for parents to manage approvals efficiently.
5. Lay the foundation for future security enhancements, including ad-blocking, malware protection, and additional parental control features.

The project aims to empower parents with better oversight of their children's digital spending habits by achieving these objectives while ensuring a safer and more controlled online experience.

5. METHODOLOGY

This project aims to develop a parental control system that, **Implements Real-Time Transaction Authorization, Integrates Advanced Threat Detection**, and **Provides a Centralized Monitoring Dashboard**. The initial version of the framework is proposed as shown in figure 1.

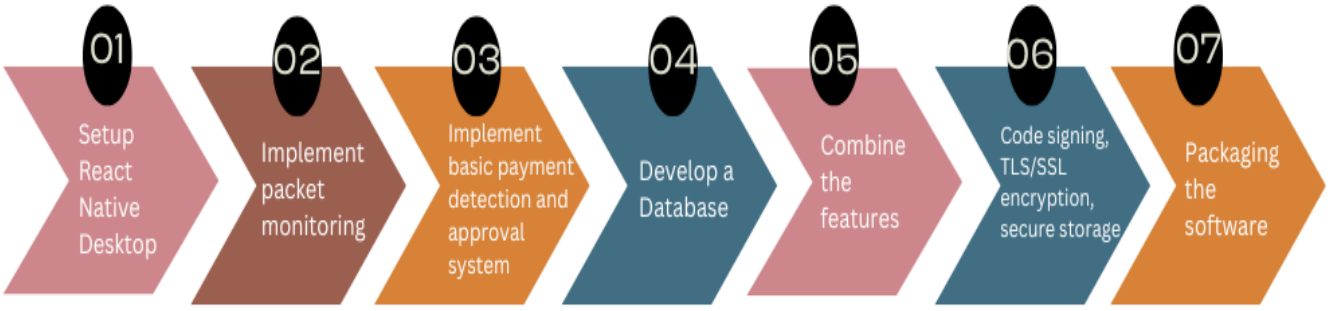

Figure .1: Proposed Methodology

6. PROJECT TIMELINE

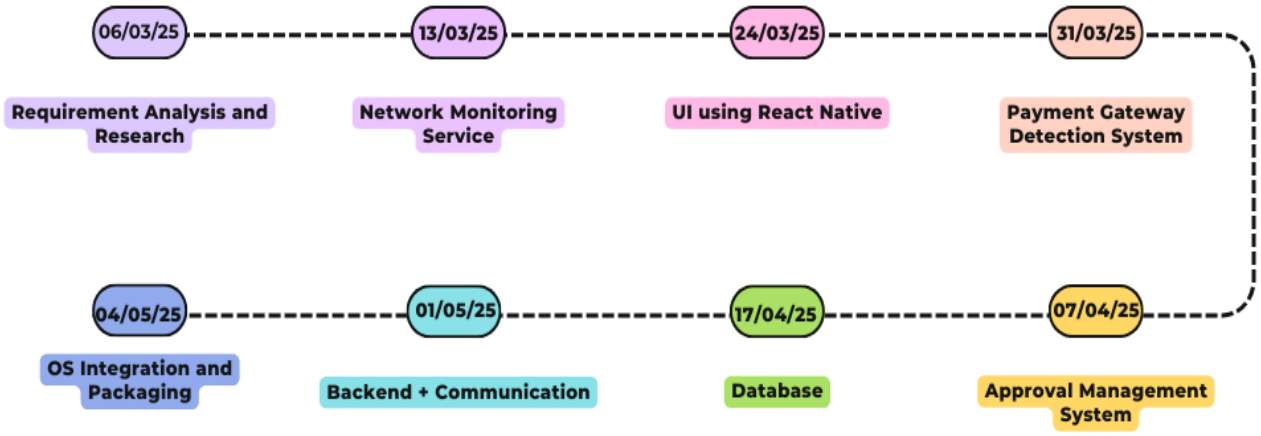

Figure 2: Project Timeline

REFERENCES

1. "Federal Court Finds Amazon Liable for Billing Parents for Children's Unauthorized In-App Charges", Press Release Reference url: "https://www.ftc.gov/news-events/news/press-releases/2016/04/federal-court-finds-amazon-liable-billing-parents-childrens-unauthorized-app-charges" dated April 27, 2016 , accessed on Feb 25, 2025.
2. Moti, Zahra, et al. "Targeted and troublesome: Tracking and advertising on children's websites." 2024 IEEE Symposium on Security and Privacy (SP). IEEE, 2024.
3. "Rise in scam job texts to teens from fraudsters posing as TikTok staff, study finds" by Shane Hickey, url: "https://www.theguardian.com/money/2025/feb/05/rise-in-scam-job-texts-to-teens-from-fraudsters-posing-as-tiktok-staff-study-finds?CMP=share_btn_url" dated Feb 5, 2025, accessed on Feb 25, 2025.

Student's Signatures **Mentor's Signature**

1) Ankit Kumar Singh (22bcs015)

2) Apiksha (22bcs020) (Dr. Rohit Tanwar)

3) Soumitra Rai (22bcs090)