#### Project report on

**Mobile Device Profiling and Tracking**

**A Dissertation submitted in partial fulfillment of the Academic requirements for the award of the degree of**

**Bachelor of Technology**

## In

**Computer Science & Engineering (Cyber Security)**

**Submitted by**

Prasanna kumari (22H51A6241)

S.Sadhana (22H51A6244)

J. Tara Sri Nikhila (22H51A6253)

**Under the esteemed Guidance of**

 **Dr.R.Venkateswara Reddy (Associate Professor and HOD,CSC)**

**Department of Cyber Security**

**CMR COLLEGE OF ENGINEERING & TECHNOLOGY**

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

#### CMR COLLEGE OF ENGINEERING & TECHNOLOGY

**(Autonomous)**

**(NAAC Accredited with ‘A+’ Grade & NBA Accredited) (Approved by AICTE, Permanently Affiliated to JNTU Hyderabad)**

**KANDLAKOYA, MEDCHAL ROAD, HYDERABAD-501401**

**DEPARTMENT OF CYBER SECURITY**



#### CERTIFICATE

This is to certify that the Mini Project -1 report entitled “**Mobile Device Profiling and Tracking**” being submitted by **Prasanna kumari(22H51A6241), Sadhana(22H51A6244), J.Tara sri Nikhila(22H51A6253)** in partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)** is a record of bonafide work carried out his/her under my guidanceand supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree.

M.Uma Maheswara Rao Dr. R. Venkateswara Reddy

Assistant Professor Associate Professor & HOD

Dept. of CSC Dept. of CSC

#### ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express my heartfelt gratitude to all the people

`who helped in making this project a grand success.

I am grateful to **M.Uma Maheswara Rao**, Assistant Professor, Dept. of Computer Science and Engineering for her valuable suggestions and guidance during the execution of this project.

I would like to thank **Dr. R. Venkateswara Reddy**, Head of the Department of Computer Science and Engineering, for his moral support throughout the period of my study in CMRCET.

I am highly indebted to **Major Dr. V.A. NARAYANA**, Principal CMRCET, for giving permission to carry out this project in a successful and fruitful way.

I would like to thank the Teaching & Non- teaching staff of the Department of Computer Science and Engineering for their co-operation.

Finally, I express my sincere thanks to **Mr. CH. GOPAL REDDY**, Secretary, CMR Group of Institutions, for his continuous care. I sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project work.

Prasanna kumari (22H51A6241)

Sadhana (22H51A6244)

J.Tara Sri Nikhila (22H51A6253)

#### ABSTRACT

* Storm Breaker is a cutting-edge, AI-driven mobile network security solution designed to simulate advanced threats and fortify defenses for ethical hackers and security professionals. This innovative platform leverages machine learning algorithms to identify vulnerabilities, detect anomalies, and predict potential threats, empowering users to proactively strengthen their mobile networks. With Storm Breaker, users can conduct realistic penetration testing, vulnerability assessments, and security audits to ensure the integrity of their mobile infrastructure. The solution's user-friendly interface and customizable scenarios enable precise simulations of real-world attacks, allowing security professionals to refine their skills and develop proactive strategies. By harnessing the power of Storm Breaker, organizations can transform their mobile network security, safeguard sensitive data, and stay ahead of emerging threats.

**Table Of Content**

|  |  |  |
| --- | --- | --- |
| **CHAPTERS** | **DESCRIPTION** | **PAGE NUMBERS** |
| 1 | INTRODUCTION | 2 |
| 1.1 | AIM | 3 |
| 1.2 | SCOPE | 4 |
| 2 | LITERATURE REVIEW | 6 |
| 3 | EXISTING SOLUTIONS | 8 |
| 4 | PROPOSED SYSTEM | 10 |
| 4.1 | REQUIREMENT ANALYSIS | 11 |
| 4.1.1 | HARDWARE REQUIREMENTS | 11 |
| 4.1.2 | SOFTWARE REQUIREMENTS | 11 |
| 4.2 | MERITS AND DEMERITS | 12 |
| 5 | DESIGN DESCRIPTION | 15 |
| 5.1 | CONCEPTUAL DESIGN | 15 |
| 6 | IMPLEMENTATION AND DISCUSSION | 17 |
| 6.1 | IMPLEMENTATION | 17 |
| 7 | RESULT | 20 |
| 8 | CONCLUSION AND FUTURE ENHANCEMENT | 21 |
| 8.1 | CONCLUSION | 21 |
| 8.2 | ENHANCEMENT | 21 |
| 8.3 | REFERENCES | 24 |

#### 

# CHAPTER 1

#### INTRODUCTION

#### The field of ethical hacking and penetration testing has emerged as a crucial component of mobile network security. Ethical hackers and security professionals use various tools and techniques to simulate attacks, identify vulnerabilities, and strengthen mobile networks. However, existing solutions often fall short in providing realistic threat simulations, advanced vulnerability detection, and user-friendly interfaces.Storm Breaker aims to address these limitations by providing a revolutionary mobile network security solution that leverages AI-powered threat simulation, advanced vulnerability detection, and a user-friendly interface. By harnessing the power of Storm Breaker, organizations can transform their mobile network security, safeguard sensitive data, and stay ahead of emerging threats.

#### AIM

* + The aim of our project is to **Mobile Device Profiling and Tracking** by sending a random link to the mobile phone to access network and data of that mobile to improve network operations and user experience.
* the project will demonstrate the scalability and efficiency of Storm Breaker technology, showcasing its ability to handle large volumes of data generated by modern mobile networks without compromising performance or security.
* Educate users and developers about the importance of robust security measures in mobile applications and web services, particularly concerning data privacy and protection.
* Utilize Storm Breaker to enable seamless and secure access to sensitive data from mobile devices, including camera, microphone, location, and device details.

#### SCOPE

* Developing scripts and configurations to demonstrate data access capabilities for camera, microphone, location, and device details.
* Identifying and showcasing potential security vulnerabilities associated with unauthorized data access through phishing links and insecure connections.
* Providing a user interface to interact with captured data, demonstrating real-time access and processing capabilities.
* Potentially contributing insights and outcomes to academic or technical publications to advance knowledge in cybersecurity.

#### 

# CHAPTER 2

#### 

#### 2.1 LITERATURE REVIEW

1. **“A Systematic Review on Security and Privacy Issues in Mobile Devices and Systems"**

**Authors:** Kitchenham.B, Pearl Brereton.O, Budgen.D, Turner.M, Bailey.J, Linkman.S.

**Journal:** Information and Software Technology.

**Year:** 2019

This paper reviews the prevalent security and privacy concerns associated with mobile devices. It discusses tools and techniques like Drozer that are used to identify and mitigate vulnerabilities in mobile applications. It discusses theoretical frameworks and potential implementations similar to Storm Breaker.

1. **"A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions"**

**Authors:** Ibrahim Tariq Javed, Kashif Naseer Qureshi, Moazam Ali, Noel Crespi

**Journal**: Applied Sciences

**Publication Year:** 2022

This paper evaluates the performance of web application vulnerability scanners by testing them on deliberately vulnerable applications. It highlights the strengths and weaknesses of different security scanners and emphasizes the importance of automated penetration testing to reduce the time, cost, and resources required for securing web applications​

# CHAPTER 3

#### 1EXISTING SOLUTION

1. **Metasploit Framework:**The Metasploit Framework is a powerful open-source tool for developing, testing, and executing exploits against various systems, including mobile devices. It includes a vast library of exploits, payloads, and auxiliary modules that can be used for penetration testing.



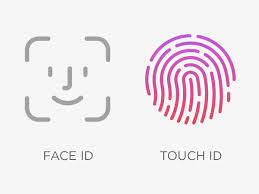
**Fig 1: Metasploit Framework**

##### Drozer: Drozer is a security assessment framework for Android that focuses on identifying and exploiting vulnerabilities in Android applications. It allows security testers to interact with applications and the underlying Android operating system to perform various security assessments.

##### DROZER – Android Security Assessment Framework

**FIG 2: Drozer**

1. **Apple Face ID and Touch ID**: Apple's Face ID and Touch ID technologies provide biometric authentication on iPhones and iPads, offering secure and convenient access to devices and apps while protecting user privacy.



**Fig 3:Apple Face and Touch ID**

# 

#### 

#### CHAPTER 4

#### 4.1.PROPOSED SYSTEM

* The exponential growth in mobile device usage has revolutionized data access but also introduced significant security challenges. Traditional security mechanisms, such as static firewalls and basic encryption techniques, struggle to keep pace with the dynamic and complex nature of mobile networks and often lack comprehensive integration and systematic security measures, leading to vulnerabilities and inefficiencies. Existing solutions often require disjointed setups and lack centralized control, posing risks to data integrity and user privacy. Moreover, as mobile applications become more prevalent, the attack surface expands, making it increasingly difficult to safeguard sensitive information. The emergence of advanced persistent threats (APTs) and sophisticated malware targeting mobile platforms exacerbates these security concerns, highlighting the need for more robust and adaptive security solutions.
* The "Storm Breaker" methodology addresses these challenges by offering a cohesive and streamlined approach to mobile data access and network security. By leveraging Kali Linux, secure tunneling with ngrok, and an integrated setup process, "Storm Breaker" provides a comprehensive solution that enhances data integrity and security. It ensures user consent and compliance with legal and ethical standards, thereby mitigating potential legal risks associated with unauthorized data access. Furthermore, the systematic steps involved in deploying "Storm Breaker" facilitate easier management and monitoring of mobile data, reducing the likelihood of security incidents and improving overall operational efficiency. In essence, "Storm Breaker" not only enhances security and data integrity but also facilitates ethical and legal compliance, providing a superior solution for mobile data access and network security.

#### REQUIREMENT ANALYSIS

##### 4.2.1 Software Requirements

* + - * Kali Linux
      * Firefox,chrome
      * Storm-Breaker
      * ngrok

##### 4.2.2 Hardware Requirements

* Mobile phone



Fig 4 :Kali Linux Fig 5:ngrok

##### 4.3 MERITS AND DEMERITS Merits:

* + - * Enhanced Data Access Capability
      * Improved Efficiency
      * Security Enhancement
      * Educational and Awareness Value
      * **Flexibility and Accessibility**

##### Demerits:

* + - * Privacy Concerns
      * Risk of Misuse

#### CHAPTER 5

#### 5.1 DESIGN DESCRIPTION

##### 5.1.1 CONCEPTUAL DESIGN

The diagram shows the steps involved in Access Mobile Network And Data Security(AMND)

**Fig 6:** Steps for VAPT

**Fig 6**: Steps for AMND

# CHAPTER 6

#### 

#### 1.IMPLEMENTATION AND DISCUSSION

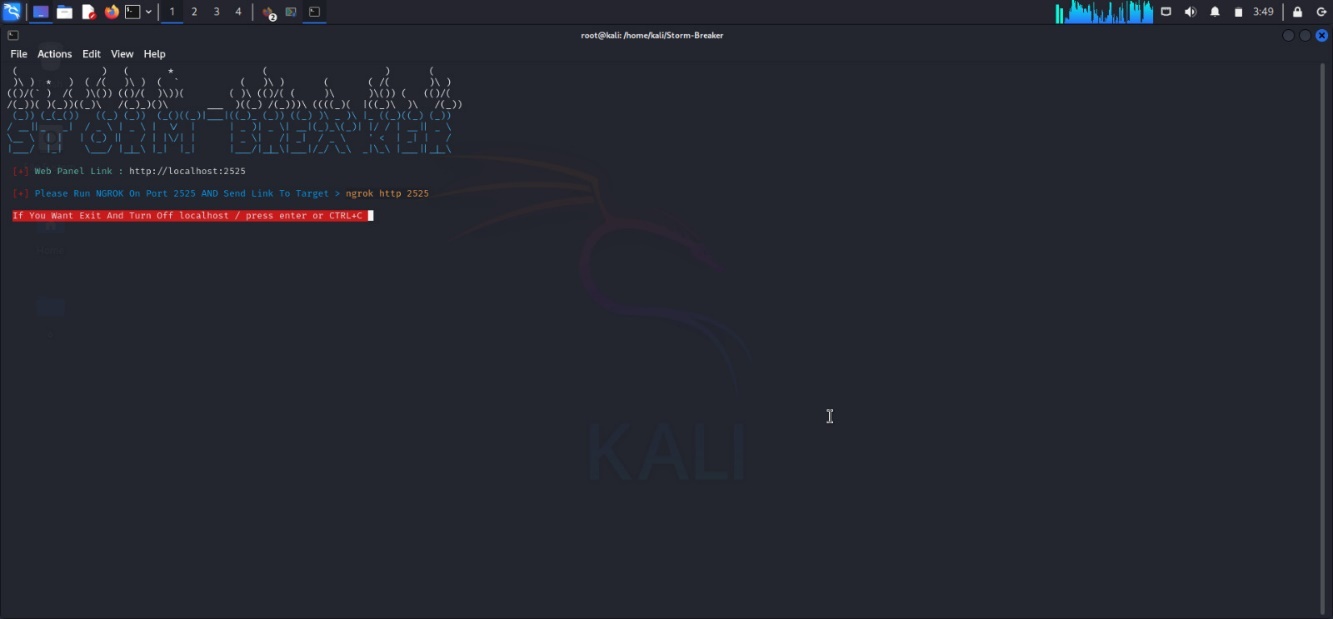
* 1. **IMPLEMENTATION**

**Setup the environment**:

Use Kali Linux or a suitable platform for testing and deploying "Storm Breaker." Install necessary software dependencies and libraries required for the project, ensuring compatibility and functionality.

### COMMAND: 1.cd Storm-Breaker

### 2. Python3 st.py



**Fig 7: Storm-Breaker**

* Signup in ngrok website and install in kali linux and add the configure it in the terminal

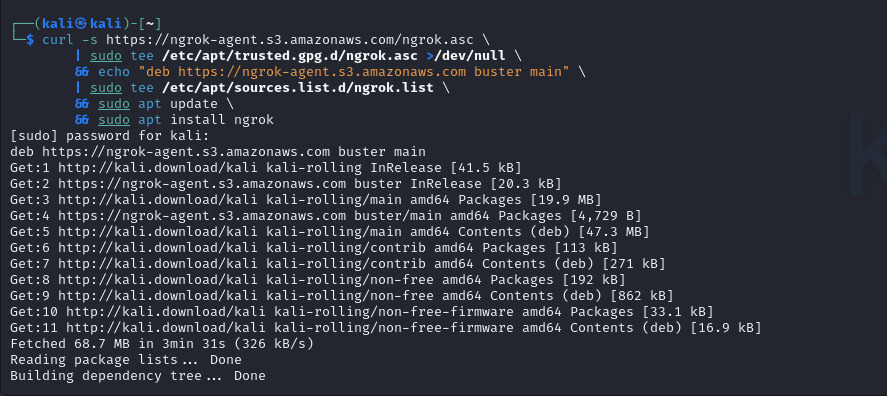


Fig 8: ngrok installation

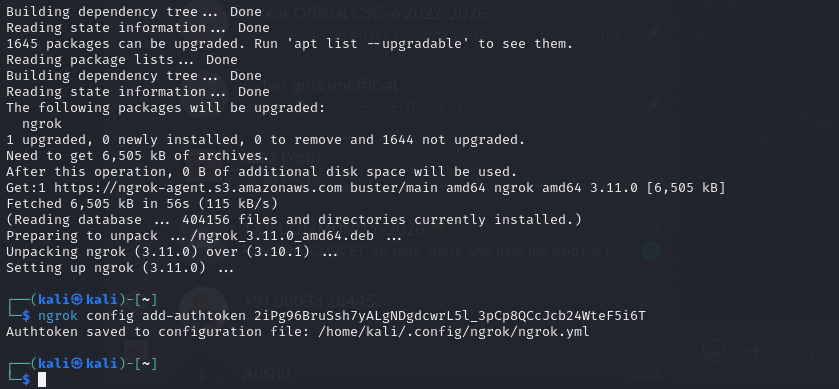


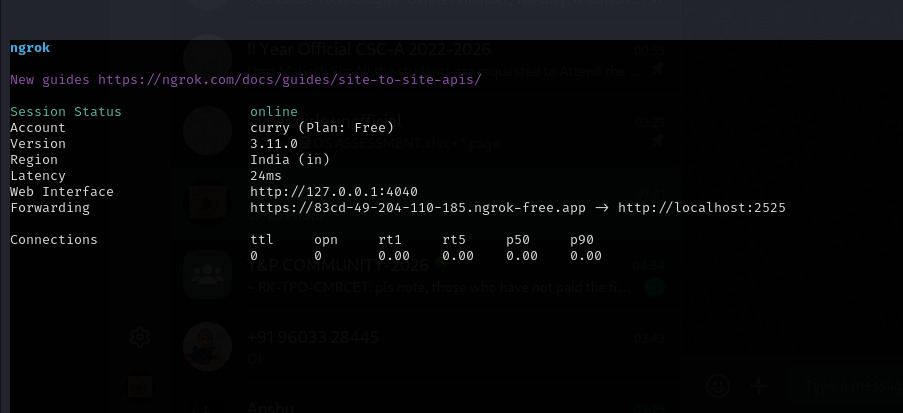
Fig 9 : ngrok config

**COMMAND: ngrok http 2525**

Click on the forwarding link it will direct to storm-Breaker website

**Fig 9:**ngrok config

13



**Fig 10 : forward link**

Link is generated now forward it to any mobile as an application http://83cd-49-204-110-185.ngrok-free.app/templates/camera\_temp/index.html

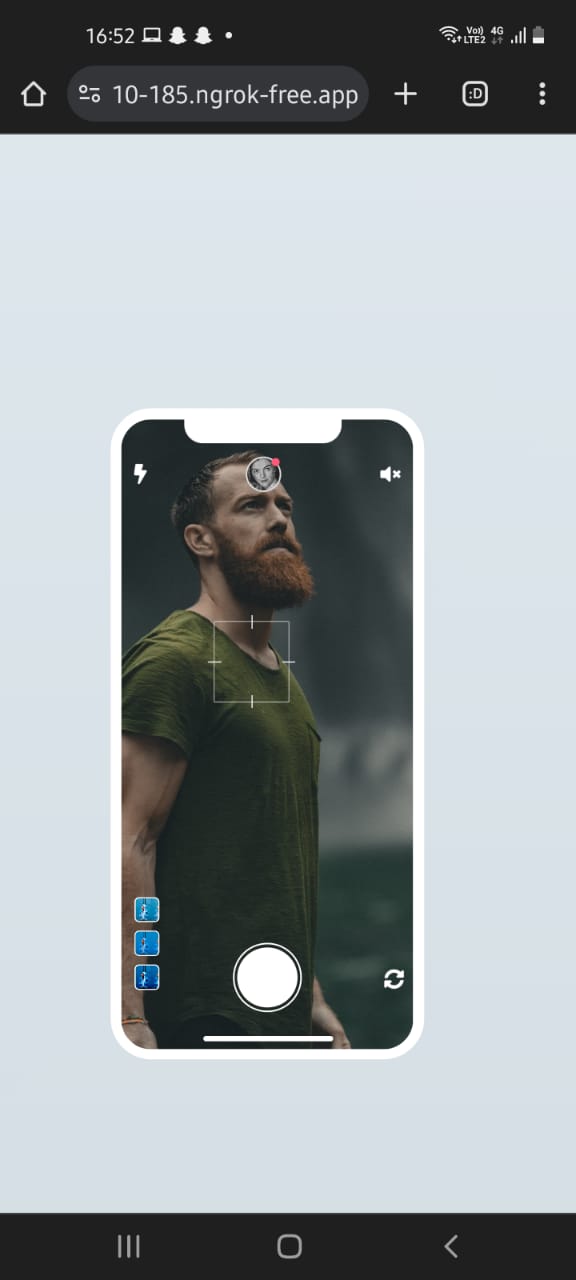


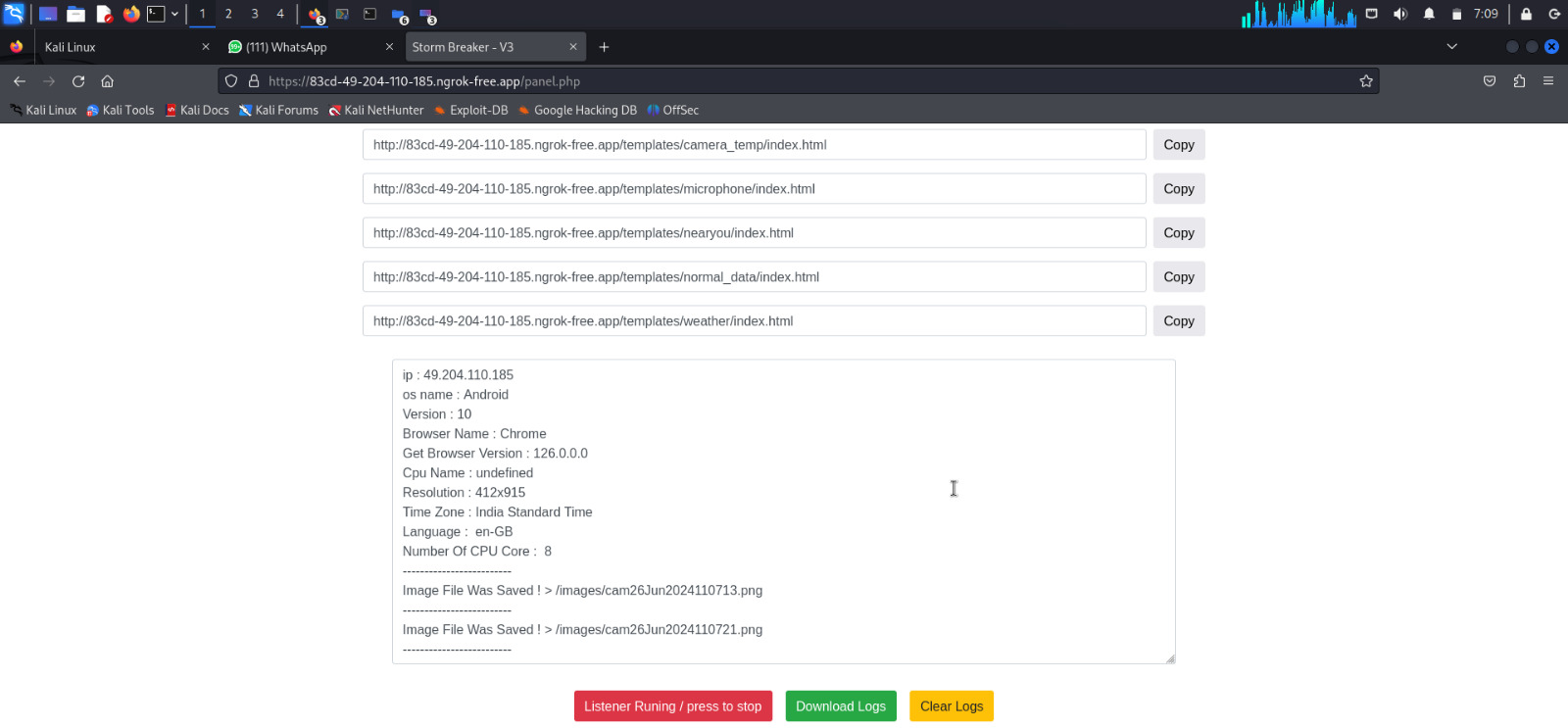
Fig 11 : face app

14

**CHAPTER 7**

#### 7.1 RESULT

we have successfully gained the access of the mobile. Now we can get the camera,microphone and location and the network device configuration details



**Fig 12: output**

15

# CHAPTER 8

#### 8.1.CONCLUSION AND FUTURE ENHANCEMEMT

##### 8.1.1 CONCLUSION

The methodology for using "Storm Breaker" to access mobile data and ensure network security represents a significant advancement over traditional methods. By leveraging Kali Linux, secure tunneling with ngrok, and a streamlined setup process, it provides a more cohesive and robust framework for data transmission and security. This approach ensures user consent and compliance with legal and ethical standards, addressing the vulnerabilities and inefficiencies inherent in existing solutions. By integrating these systematic steps, "Storm Breaker" not only enhances data integrity and security but also simplifies the process of accessing and managing mobile data. Consequently, it offers a superior, more secure, and ethical solution for mobile data access and network security.

##### 8.1.2 FUTURE ENHANCEMENTS

* **Advanced Authentication**: Integrate biometric authentication and granular role-based access control.
* **AI and Machine Learning**: Implement anomaly detection and predictive analysis for proactive security.
* **End-to-End Encryption**: Ensure comprehensive encryption for data in transit and at rest, with secure storage solutions.

16

#### 8.2REFERENCES

1. OWASP Foundation. (2021). OWASP Secure Coding Practices - Quick Reference Guide.
2. McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley Professional.
3. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
4. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
5. Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.

17