Trusted GPT-4, ChatGPT and AI Detector tool by ZeroGPT

ZeroGPT the most Advanced and Reliable Chat GPT, GPT4 & AI Content Detector

AI/GPT Detector | ZeroCHAT-4 & 5 | AI Text Summarizer | AI Paraphraser | AI Grammar & Spell Checker | Word Counter

```
Web app for detecting Malicious and fraudulent
activities over Social Networking Sites


A PROJECT REPORT


Submitted by

Saumya Sharma
20BCS6224
```

Detect Text | Upload File | 14,999/15,000 Characters (Get up to 100,000 here)

Web app for detecting Malicious and fraudulent activities over Social Networking Sites

A PROJECT REPORT

Submitted by

Saumya Sharma
20BCS6224

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING IN
COMPUTER SCIENCE WITH SPECIALIZATION IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING & INFORMATION SECURITY

Under the Supervision of:
Mr. Ankit Garg

CHANDIGARH UNIVERSITY, GHARUAN, MOHALI - 140413, PUNJAB
December, 2023

i

BONAFIDE CERTIFICATE

Certified that this project report “Web app for detecting Malicious and fraudulent
activities over Social Networking Site s”
is the bonafide work of “ Saumya Sharma ” who carried out the project work under my/our supervision.

SIGNATURE
Mr. Ankit Garg

HEAD OF THE DEPARTMENT
SIGNATURE

SUPERVISOR

Submitted for the project viva -voce examination held on

INTERNAL EXAMINER EXTERNAL EXAMINER

ACKNOWLEDGEMENT

No project is ever complete without the guidance of those expert who have already traded this
past before and hence become master of it and as a result, our leader. So, I would like to take this
opportunity to take all those individuals how have helped me in visualizing this project.

I would take this opportunity to thank our Major Project Supervisor “Ankit Garg ” and Evaluation
panelists “ Mr. Dayal Chandra Sati ” and “Mr. Gaura v Soni ” for their guidance in selecting this
project and also for providing timely assistant to my query and guidance of this project.

I extend my sincere appreciation to our Project Supervisor for providing me the opportunity to
implement the project.

I am really thankful to all our Professors from AIT-CSE (Chandigarh University)

for their
valuable inside and tip during the designing of the project. Their contributions have been
valuable in so many ways that I find it difficult to acknowledge every of them individually.

Thank You

ABSTRACT

In the digital age, the recent years, the continuous growth of social networking sites such as
Facebook, Instagram, whatsapp has expanded the online communication throughout the world.
These platforms provide seamless interaction and keep us up to date with the current world but these
have some dark sides too. These platforms are become the major source for malicious and the
fraudulent activities.
The subsequent nature of social networking has surged the online communication which is enabling
the world to socially get updated and be connected all over the world, however, this convenience
has also given rise to a disturbing trend: fake video calls l eading to potential blackmail. So, the key

features of our proposed web app includes monitoring the unknown callers, alerting mechanisms
and reporting capabilities offering user an adaptive and protective defense mechanism for the
privacy, security and saf ety.
The proposed web application is used for detecting and investigating the malicious and fraudulent
activities on the social networking sites represents a significant advantage in the ongoing efforts to
enhance the online security. Through timely alerts and intervention, the web application empowers
users to take control of their digital security. This research not only examines the growing risks
through fake video calls on social platforms but also offers some practical solutions to mitigate these
threats.

Basically, this web app does the work of cyber security first it will detect the unknown number, cross
– verify it through the multiple platforms, like the username on UPI apps, social platforms, truecaller
and then matches the result and reports to the us er if found suspected. The increasing prevalence of
malicious and fraudulent activities on social networking sites poses significant challenges in
maintaining a secure and trustworthy online environment. This project introduces a web application
designed t o detect and mitigate such activities, contributing to enhanced user safety and a more
secure online community.

The goal of strengthening internet security and equipping users with a strong

defense against
blackmailing attacks is improved by the research. They cybersecurity community as well as end -
users can benefit from the study's findings and ideas. Future work may involve further model
improvements, continuous monitoring, and adaptation to changing threats. 1

CHAPTER 1
INTRODUCTION

1.1 Background Information

The explosive growth of social networking sites over the past decade has fundamentally transformed the way
individuals communicate, share information, and connect with others across the globe. Platforms such as
Facebook, Twitter, Instagram, and LinkedIn have become integral parts of daily life, facilitating the exchange
of ideas, fostering communities, and serving as hubs for both personal and professional networking. However,
this unprecedented connectivity comes with a dark underbelly – the proliferation of malicious and fraudulent
activities that threaten the very essence of these online communities. As users engage in a n ever -expanding
digital ecosystem, the vulnerabilities within social networking sites become apparent.

Malicious actors exploit the trust and openness inherent in these platforms, perpetrating a range of activities that
compromise user privacy, disseminate false information, and jeopardize the integrity of online interactions.
Phishing attempts, account compromises, and the intentional spread of misinformation have emerged as
formidable challenges, requiring novel and sophisticated solutions to s afeguard

the digital landscape. In this
context, the motivation behind the development of an Android application for detecting malicious and fraudulent
activities is rooted in a commitment to address these growing concerns. As the prevalence of online thre ats
continues to escalate, there is an urgent need for tools that not only respond to existing challenges but also
anticipate and prevent future risks.

This project seeks to provide a holistic solution that combines technological innovation, machine learning
algorithms, and community engagement to fortify social networking platforms against the evolving landscape
of online threats. The convergence of technology and human interaction within the realm of social networking
sites underscores the significance of proactive measures in securing the digital space. By delving into the
intricacies of user -generated content, interaction pattern s, and network behavior s, this Android application aims
to disrupt the strategies employed by malicious entities.
Furthermore, the project recognizes the indispensable role of user collaboration in the ongoing battle against
online threats, placing emphasis on empowering individuals to actively contribute to the collective security of
the digital community. In the subsequent sections, we will explore the intricacies of the Android application's
development, methodology, and outcomes. By understanding the background of the project, we lay the
foundation for a comprehensive examination of how technology and com munity co llaboration can work
synergistically to create a safer, more secure online environment.

1.2 Identification of Problem

The advent of social networking sites has revolutionized the way people connect and share information,
fostering a globalized digital community. However, the widespread adoption of these platforms has given rise
to a myriad of security challenges, with malicious and fraudulent activities emerging as significant threats to the
integrity of online interactions.

Phishing attacks pose multiple challenges due to their multidimensional nature:
• Phishing Attempts : Social networking sites often serve as breeding grounds for phishing
attempts, where malicious entities impersonate trusted individuals or organizations to
deceive users into revealing sensitive information. These deceptive practices compromise
user privac y and can lead to financial or identity theft.
• Account Compromise : The unauthorized access to user accounts represents a persistent
and escalating issue. Malicious actors employ various techniques, including password
breaches and social engineering, to compromise user accounts. Once infiltrated, these
accounts can be used for fraudulent activities, spreading misinformation, or launching
further attacks.
• Dissemination of Misinformation : The rapid dissemination of information on social
networking sites makes them susceptible to the intentional spread of misinformation.
False narratives, fake news, and manipulated content can rapidly gain traction, contributing to a climate of distrust and confusion.

• Inadequate Reporting Mechanisms : Existing reporting mechanisms on social platforms
may lack effectiveness, leading to delayed or insufficient responses to identified threats.
Users may encounter challenges in reporting suspicious activities, hindering the collective
effort to maintain a s ecure online environmen t.
• Dynamic Nature of Threats: The evolving landscape of online threats requires a dynamic
and adaptive approach to detection. Traditional security measures may struggle to keep
pace with the ever -changing tactics employed by malicious actors, necessitating innovative solutions.

The identification of these problems underscores the need for a comprehensive and proactive system
capable of detecting and mitigating malicious and fraudulent activities on social networking sites. 3
As users increasingly rely on these platforms for personal and professional interactions, addressing
these challenges becomes imperative to uphold the trust, security, and integrity of the digital
community. In response to these identified issues, this pro ject aims to develop an Android
application that combines advanced technological solutions with user engagement to fortify social
networking sites against the spectrum of online threats , legitimate and malicious URLs, thereby
enhancing online security and reducing the risks associated with phishing attacks.

1.3 Identification of Tasks

1. Literature R eview
Conduct a thorough literature review on existing research, tools, and methodologies related to the detection of
malicious and fraudulent activities on social networking sites. Summarize key findings and identify gaps in
current knowledge.
2. Problem Statement Definition
Clearly define and articulate the problem statement, highlighting the specific challenges associated with
malicious activities on social platforms that the Android application aims to address.
3. Objective Formulation
Clearly outline the objectives of the Android application, specifying the goals related to detection mechanisms,
user engagement, and overall enhancement of online security.
4. Methodology Design
Clearly outline the objectives of the Android application, specifying the goals related to detection
mechanisms, user engagement, and overall enhancement of online security.
5. Methodology De sign
Design the methodology section detailing the technical approach of the Android application. Specify the
machine learning algorithms, data preprocessing techniques, and integration methods with social networking
APIs.
6. Data Collection Plan
• Develop a plan for data collection, specifying the sources of data, data types, and any
preprocessing steps required to ensure the quality and relevance of the dataset.

1.4 Timeline

Creating a timeline for a project report involves estimating the time required for each task and organizing them
in a logical sequence .

Days 1 -2: Project Kickoff
Set up project environment, organize files, and initiate version control if applicable.

Days 3 -7: Literature Review
Begin the literature review, focusing on existing research, tools, and methodologies related to
detecting malicious activities on social networking sites.

Days 8 -10: Problem Statement and Objectives
Define the problem statement and clearly outline the objectives of the Android application.

Week 3 -4: Methodology and Data Collection

Days 11 -12: Methodology Design
Design the methodology section, specifying the machine learning algorithms, data preprocessing
techniques, and integration methods.

Days 1 3-15: Data Collection Plan
Develop a plan for data collection, specifying sources, types of data, and preprocessing steps.

Days 18 -21: System Architecture Design

Create a comprehensive system architecture diagram.

Week 4-5: Android App Implementation and UI Design

Days 22 -24: Android App Implementation
Begin coding the Android application, incorporating the designed architecture and methodology.

Days 2 5-30: User Interface Design
Design an intuitive and user -friendly interface for the Android application. 5
Week 6: Preliminary Testing and Results Implementation

Days 3 1-37: Preliminary Testing
Conduct preliminary testing to identify and address any initial issues or bugs.

Days 38-45: Results and Evaluation Section
Implement the results and evaluation section, presenting outcomes and relevant metrics.

Week 8: Discussion, Conclusion, and Future Scope

Days 46-50: Discussion of Results and Conclusion
Analyze and discuss results; draft the conclusion section summarizing key findings.

Days 5 1-55: Future Scope Section
Outline the future scope of the project, identifying potential areas for improvement and expansion.

Week 9: Abstract, Introduction, and Review/Edit

Days 56-61: Abstract Writing
Write the abstract, providing a concise summary of the entire report.

Days 62-66: Introduction Drafting
Draft the introduction section, providing background information and introducing the Android
application.

Days 67-72: Review and Edit
Review and edit the entire report for coherence, clarity, and adherence to academic writing standards.

Week 10: Formatting, Appendices, Presentation Preparation

Days 68-75: Formatting and Styling
Format the report according to guidelines, including proper citation styles.

6
Days 76-85: Appendices and Supplementary Materials
Compile supplementary materials into appendices as needed.

Days 86-92: Presentation Preparation
If required, prepare a slide deck summarizing key points of the report for a presentation.

Week 11: Final Review and Submission

Days 93-100: Final Review
Perform a final review of the report, checking for any remaining errors or inconsistencies.

Chapter 1 – Introduction

It will include the Background information, Identification of Problem, Identification of Tasks &

Highlighted text is suspected to be most likely generated by AI*

14,999 Characters

2,019 Words

Simple and Credible Open AI and Bard detector tool for Free

Millions of users trust ZeroGPT, See what sets ZeroGPT apart

Highlighted Sentences

Every sentence written by AI is highlighted, with a gauge showing the percentage of AI inside the text

Batch Files Upload

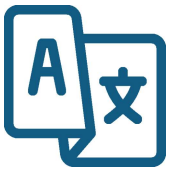
Simply upload multiple files at once, and they will get checked automatically in the dashboard

High Accuracy Model

Advanced and premium model, trained on all languages to provide highly accurate results

Generated Report

Automatically generated .pdf reports for every detection, used as a proof of AI-Free plagiarism



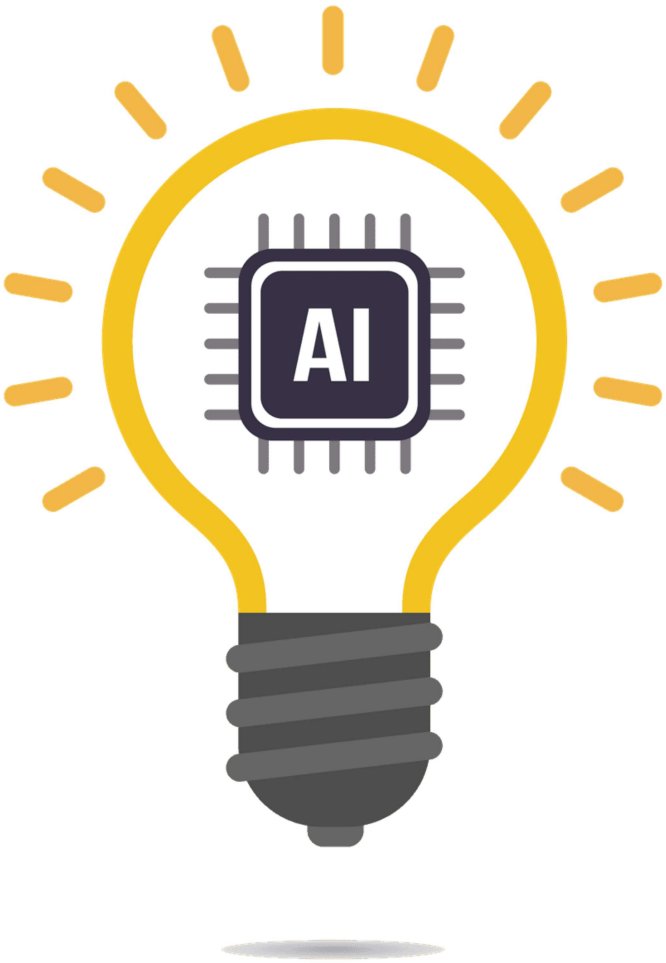
Support All Languages

Support all the languages with the highest accuracy rate of detection

GET PREMIUM FEATURES

Unlock growth potential with our API

Our team has developed a user-friendly API for organizations. Get API access



DeepAnalyse™ Technology

A pioneering research in the modeling of AI content detection

Our AI detection model includes several components that analyze text to determine its origin and if it was written by AI. We use a multi-stage methodology designed to optimize accuracy while minimizing false positives and negatives. From the macro level to the micro one, this is how DeepAnalyse™ Technology works. Our model specializes in identifying AI generated content like Chat GPT, GPT 3, GPT 4, Bard, LLaMa models ...
Finally, we employ a comprehensive deep learning methodology, trained on extensive text collections from the internet, educational datasets, and our proprietary synthetic AI datasets produced using various language models.

Explore More Tools to Enhance Your Writing Skills

Fix grammar and spelling mistakes, detect AI plagiarism, check for plagiarism, generate citations, advanced word counter, powerful summarizer and paraphraser

- Advanced AI ChatBot
- AI Grammar Checker
- AI Summarization Tool
- AI Paraphrasing Tool
- Word Counter Tool

Your questions, answered

How Does ZeroGPT work?

What is the accuracy rate of ZeroGPT?

Who Benefits from ZeroGPT's AI content detector?

Will my text get plagiarized or be available online, if I check it on ZeroGPT?

How can I integrate ZeroGPT tool in my organization or website on a large scale?

Does ZeroGPT work with different languages?

How can I cite the detector?

A set of products to help you do more

SendBig

Quickly and Securely deliver large files—up to 30 GB for Free—to anyone. Unique features, detailed dashboard, ISO Certified service and a fully customizable experience

Learn more →

Unreal Person

The most advanced AI image generator for Human, Cat, Horse and Art. With UnrealPerson, generate Fake images with AI that looks 100% real but they don't exist in reality!

Learn more →

Pomonow

The famous Time Management method that Boosts your Productivity while working or studying... It is PomoNow, one of the popular time management hacks used today

Learn more →

WaterOutPhone

The easiest way to eject water, remove dust and fix your speaker by playing verified sound.

Learn more →

Check Our Blog created with the help of AI

5 Mind Blowing Technologies we'll see in 2023
10 Ridiculous Technologies That Will Actually Make Your Life Better

More about

Pricing

Our policy

Terms of use

Features

AI Detector

AI ZeroChat-4 & 5

Summarizer

Paraphraser

Grammar Checker

Word Counter

Question / Business inquiry

You can email us at

support@zerogpt.com

Our support team is spread across the globe to give you answers fast