

FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING



A DESIGN PROJECT REPORT

Submitted by

PRAVEEN A	(730920104085)
RAMPRADEEP J	(730920104092)
THAMARAI SELVAN G	(730920104115)
SURIYAPRAKASH P	(730920104113)

in partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

EXCEL ENGINEERING COLLEGE(AUTONOMOUS)

ANNA UNIVERSITY: CHENNAI-600025

KOMARAPALAYAM-637303

NOVEMBER 2023

EXCEL ENGINEERING COLLEGE::KOMARAPALAYAM

ANNA UNIVERSITY : CHENNAI-600025

BONAFIDE CERTIFICATE

Certified that this project report “**FAKE SOCIAL MEDIA PROFILE DETECTION AND REPORTING**” is the bonafide work of “**PRAVEEN A(730920104085), RAMPRADEEP J(730920104092), THAMARAI SELVANG (730920104115), SURIYAPRAKASH P(730920104113)**”, who carried out the project work under my supervision.

SIGNATURE

Dr.P.C.SENTHIL MAHESH M.E.,Ph.D.,

HEAD OF THE DEPARTMENT,

Associate Professor and Head,
Department of CSE,
Excel Engineering College,
Komarapalayam-637303.

SIGNATURE

Dr. P. Kumari M.E. ,Ph.D.,

SUPERVISOR,

Associate Professor,
Department of CSE,
Excel Engineering College,
Komarapalayam-637303.

Submitted for the University Examination held on _____

INTERNAL EXAMINER

EXTERNAL EXAMINER

ACKNOWLEDGEMENT

Behind every achievement lies an unfathomable sea of gratitude to those who actuated it, without them it would never have into existence. To them, we lay word of gratitude imprinted within ourselves.

We wish our heartfelt thanks to our respected Founder and Chairman of Excel Group Institutions Prof. **Dr. A. K. NATESAN, M.Com., M.B.A., M.Phil., PhD.,** FTA and Vice Chairman **Dr. N. MATHAN KARTHICK M.B.B.S., M.H.Sc (Diabetology)** for allowing us to have the extensive use of the college facilities to do our project effectively.

We express our sincere gratitude and heartfelt thanks to the respected Principal **Dr. K. BOMMANNA RAJA Ph.D.,** for his encouragement and support to complete the project.

We would like to express our profound interest and sincere gratitude to the Associative Professor Head, Department Computer Science and Engineering Department Prof. **Dr. P.C. SENTHIL MAHESH M.E., Ph.D.,** for his encouragement and support to complete the project.

We are privileged to express our deep sense of gratitude to Project guider Associate Professor **Dr. P. KUMARI ME., Ph.D.,** who gave guidance and support throughout our work and made this as a successful project.

We would like to give our sincere gratitude and heartfelt thanks to our Project Coordinator **Mrs. J. OBURADHA M.E.,** Department of Computer Science and Engineering, who gave guidance and support throughout my work and made this as a successful project.

Finally, we thank the Almighty, Parents, Friends, and well-wishers for the moral support throughout the project.

ABSTRACT

Our lives are significantly impacted by social media platforms such as Facebook, Twitter, Instagram, LinkedIn, and others. People are actively participating in it the world over. However, it also has to deal with the issue of bogus profiles. False accounts are frequently created by humans, bots, or computers. They are used to disseminate rumors and engage in illicit activities like identity theft and phishing. So, in this project, It will talk about a detection model that uses a variety of machine learning techniques to distinguish between fake and real Social media profiles based on attributes like follower and friend counts, status updates, and more. Using a Random Forest algorithm for detecting fake social media profiles can be an effective approach. Random Forest is an ensemble learning method that combines multiple decision trees to improve accuracy and generalization. It can be used the dataset of Social media profiles, separating real accounts into TFP and E13 and false accounts into INT,TWT, and FSF. Here, the author discusses, Random Forest.

TABLE OF CONTENT

CHAPTER NO.	CONTENT	PAGE NO
	ABSTRACT	iii
	LIST OF FIGURES	vi
	LIST OF ABBREVIATIONS	vii
1.	INTRODUCTION	1
	1.1. OVERVIEW	1
	1.2. OBJECTIVE	2
2.	LITERATURE SURVEY	3
3.	SYSTEM ANALYSIS	5
	3.1 DEMERITS OF EXISTING SYSTEM	5
	3.2 MERITS OF PROPOSED SYSTEM	6
	3.3 ARCHITECTURE	7
	3.4 USE-CASE DIAGRAMS	8
4.	MODULE DESCRIPTION	9
	4.1 REGISTRATION MODULE	9
	4.2 LOGIN MODULE	9

	4.3 DETECTION MODULE	9
5.	DESIGN AND DEVELOPMENT PROCESS	11
	5.1 VS CODE	11
	5.2 PHP	11
	5.3 HTML AND CSS	12
	5.4 JAVA SCRIPT	12
	5.5 MySQL	12
6.	IMPLEMENTATION AND RESULTS	13
	6.1 REGISTRATION PAGE	13
	6.2 LOGIN PAGE	14
	6.3 DETECTION PAGE	15
7.	CONCLUSION	16
8.	FUTURE ENHANCEMENT	17
9.	APPENDICES	18
	REFERENCE	32

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
5.2	Architecture Diagram	23
5.3	Use Case Diagram	23
5.4	Output-Registration Page	37
8.2	Output- Login Page	37
8.2	Output- Detection Page	37

LIST OF ABBREVIATION

1.	FSF :	Free Software Foundation
2.	TFP :	Total Factor Productivity
3.	SVM :	Support Vetor Machine
4.	RAM :	Random Access Memory
5.	OS :	Operating System
6.	ML :	Machine Leaning
7.	CPU :	Central Process Unit
8.	HTML	Hyper Text Markup Language
9.	CSS	Cascading Style Sheets
10.	PHP	Hyper Text PreProcessor
11.	CSV	Comma Separated Values

CHAPTER 1

INTRODUCTION

Social media plays a significant role in our lives today. Our lives nowadays rely heavily on social media. Everyone uses social media, whether it be to share beautiful, expensive photos, follow celebrities, or talk with nearby and distant pals. It is a fantastic place for exchanging knowledge and interacting with others. However, everything has a drawback. Social media has a significant role in our lives, yet there have been times when it has become problematic. Fake social media profiles, commonly known as "catfish" or "bots," can take on various forms and purposes.

False profiles are frequently made under fictitious identities, and they spread defamatory and abusive posts and images to influence society or advance anti-vaccine conspiracy theories, among other things. Phony personas are an issue on all social media platforms nowadays.

1.1 OVERVIEW

Fake social media profile detection and reporting is a significant area of research in the field of cybersecurity and digital forensics. Here's an overview based on the references you provided:

1. Machine Learning for Fake Identity Detection : This paper discusses the use of machine learning to distinguish between bots and humans, which is crucial in detecting fake identities on social media.

2. Comprehensive Review of Fake Profile Detection Techniques: This paper provides a comprehensive review of various techniques used for fake profile detection in large-scale online social networks.

3. Blacklist for Fake Account Detection: In this proposed method for detecting fake accounts on Twitter using a blacklist, demonstrating a practical application of these techniques.

4. Hybrid SVM Algorithm for Fake Profile Detection: Introduce a hybrid SVM algorithm for detecting fake profiles on social media, showcasing the potential of combining different machine learning techniques.

5. Machine Learning for Fake Profile Detection on social media: In this paper method to apply machine learning techniques to detect fake profiles on Instagram, indicating the broad applicability of these methods across different social media platforms.

These studies collectively highlight the importance and effectiveness of machine learning and artificial intelligence techniques in detecting and reporting fake social media profiles. They also underscore the ongoing need for research and development in this area to keep up with the evolving tactics of those who create fake profiles.

1.2 OBJECTIVE

The objectives of fake social media profile detection and reporting are:

1. Identifying Fake Identities: The primary objective is to accurately identify fake identities on social media platforms. This involves distinguishing between bots and humans, as well as detecting profiles that are pretending to be someone or something they're not.

2. Improving Security: By detecting fake profiles, we can enhance the security of social media platforms and protect users from potential threats. Fake profiles can be used for malicious activities such as spreading misinformation, scamming users, or carrying out cyber attacks.

3. Enhancing User Experience: Fake profiles can negatively impact the user experience on social media platforms. By detecting and removing these profiles, we can ensure that users are interacting with real individuals, which can enhance trust and engagement on the platform.

4. Informing Platform Policies and Regulations: The findings from fake profile detection can inform the policies and regulations of social media platforms. This can lead to more effective strategies for preventing the creation of fake profiles in the first place.

5. Advancing Research in Cybersecurity and Digital Forensics: This area of research contributes to the broader fields of cybersecurity and digital forensics. The techniques and methods developed can be applied to other areas, such as detecting fake news or identifying cyber threats.

CHAPTER 2

LITERATURE SURVEY

LITERATURE SURVEY 1

Title: "DETECTION OF FAKE PROFILE IN SOCIAL MEDIA"

Author: Jyoti Singh and Mohammad Zunnun Khan

Year: 2019

Journal: A Comprehensive Review. IEEE Transactions on Artificial Intelligence, 1, 271-285.

<https://doi.org/10.1109/TAI.2021.3064901>

Description: Online social networks are increasingly influencing how individuals interact with each other by exchanging their private and professional data. The social network is currently a common way to communicate with others that are spread across a variety of locations around the globe. When we speak about social networking then we can say that by sending them a request or readily sharing data with each other, anyone can readily make friends.

LITERATURE SURVEY 2

Title: " Detection of Fake Profiles on Twitter "

Author: Murthy, P.S. and Reddy, P.C.S.

Year: 2021

Journal: E3S Web of Conferences, 309, Article No. 01046.

<https://doi.org/10.1051/e3sconf/202130901046>

Description: In this comprehensive guide, we will delve into the methodologies employed in the detection of fake profiles on Twitter. From manual profile analysis and behavioral scrutiny to the application of machine learning techniques, each step is meticulously designed to enhance the accuracy and efficiency of the detection process. By understanding the nuances of fake profile creation and leveraging a combination of human intuition and technological innovation, we aim to empower users and platform administrators to mitigate the impact of deceptive profiles on the Twitter ecosystem.

LITERATURE SURVEY 3

Title: Fake Profile Identification Using Machine Learning.

Author: Oleksiy Mazhelis and Jari Veijalainen

Year: 2010

Journal: International Research Journal of Engineering and Technology (IRJET), 6, 1145- 1150.

Description: False identities play an important role in advanced persisted threats and are also involved in other malicious activities. The present article focuses on the literature review of the state-of-the-art research aimed at detecting fake profiles in social media. The approaches to detecting fake social media accounts can be classified into the approaches aimed on analyzing individual accounts, and the approaches capturing the coordinated activities

spanning a large group of accounts. The article sheds light on the role of fake identities in advanced persistent threats and covers the mentioned approaches of detecting fake social media accounts

LITERATURE SURVEY 4

Title: "The Dark Side of Social Media: Misuse of Platforms"

Author: Shalini Talwar and Puneet Kaur

Year: 2020

Journal: Wiley journals

Description: The proliferation of social media usage has led to the manifestation of certain negative behaviors that are now referred to as the 'dark side' of social media use. These behaviors are a matter of concern, as they are detrimental to people's well-being. Problematic sleep is influenced by stalking, compulsive use and poor sleep hygiene, with sleep hygiene having the strongest effect, while poor sleep hygiene and compulsive use also partially mediate the association of both stalking and online self-disclosure with problematic sleep.

CHAPTER 3

SYSTEM ANALYSIS

3.1 DEMERITS OF EXISTING SYSTEM

The existing systems for fake social media profile detection and reporting have several demerits:

- 1. Limited Factors:** The existing systems use very few factors to decide whether an account is fake or not. When the number of factors is low, the accuracy of the decision making is reduced significantly⁷.
- 2. Incompatibility for Real-Time Detection:** The machine learning algorithms used in the currently existing system, such as Random Forest, Decision Tree, and Naïve Bayes, have good accuracy but the model is incompatible to detect the fake profile in real time. It only allows the user to test on only selected dataset⁴.
- 3. Manual Procedures:** Currently, the identification of these fake profiles is limited to manual procedures. It is a tedious process and may not be sufficient due to the quality with which they can duplicate existing profiles or make compilations to create profiles bots, spammers, phishers, impersonations, or fakeaccounts³.
- 4. Challenges in Decision Making:** The challenge that promoters and marketing experts faced at the time is their scepticism about the validity of this influencer depending on a number of factors¹.

These demerits highlight the need for improved systems for fake social media profile detection and reporting.

3.2 MERITS OF PROPOSED SYSTEM

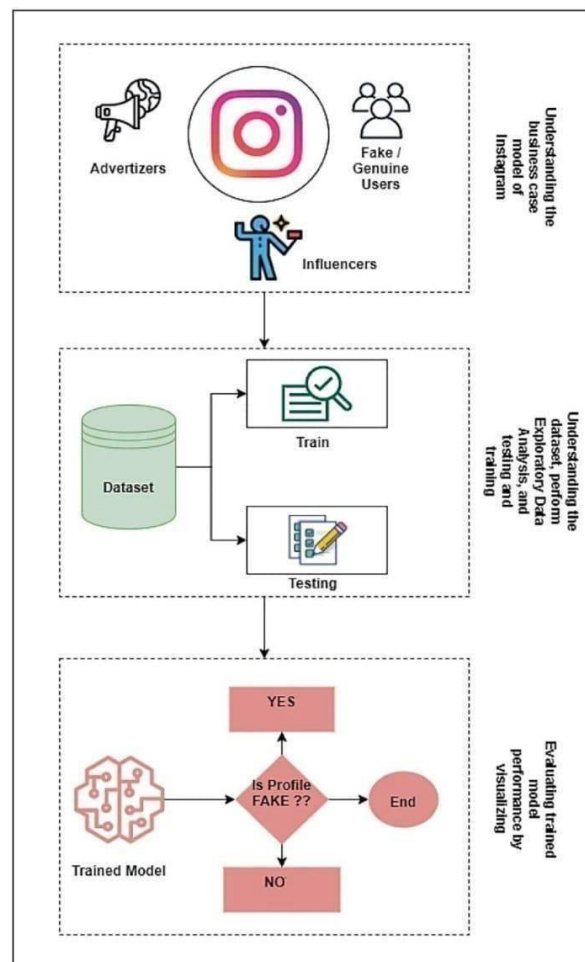
The proposed system for fake social media profile detection and reporting has several merits:

- 1. Improved Accuracy:** The proposed system can potentially improve the accuracy of fake profile detection by using advanced machine learning and deep learning techniques. This can lead to a significant reduction in the number of fake profiles on social media platforms.
- 2. Real-Time Detection:** With the proposed system, fake profiles can be detected in real-time, preventing them from causing harm or spreading misinformation.
- 3. User Trust:** By effectively detecting and reporting fake profiles, the proposed system can increase user trust in social media platforms. Users can interact on these platforms with the assurance that they are engaging with genuine profiles.
- 4. Scalability:** The proposed system can be designed to be scalable, capable of handling the large volumes of data generated on social media platforms.
- 5. Adaptability:** The system can be designed to adapt to the evolving tactics used by fake profile creators, ensuring its effectiveness over time.

Remember, the effectiveness of such a system would depend on its design and implementation, and it's important to consider potential challenges such as privacy concerns and the possibility of false positives.

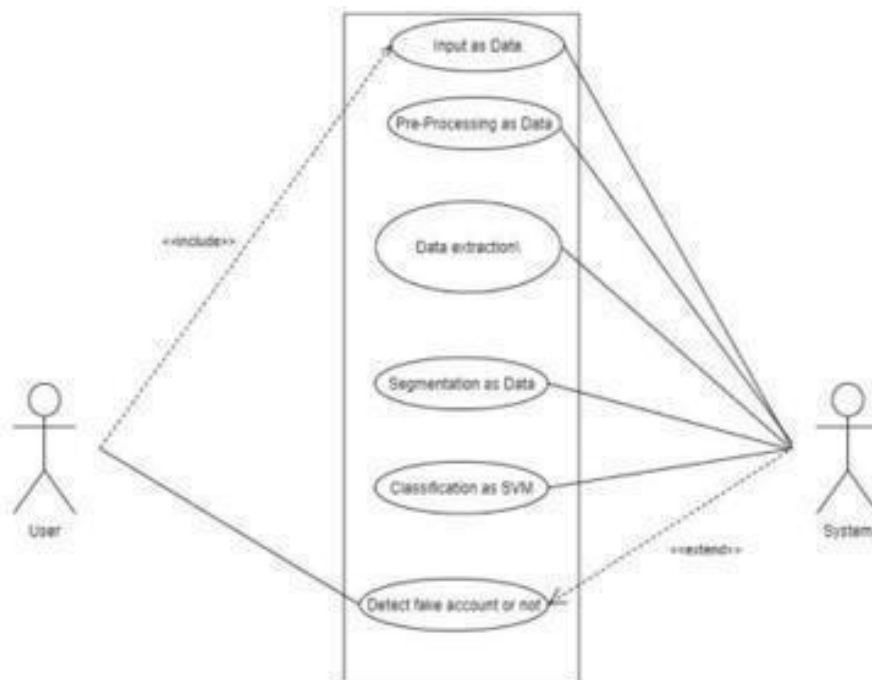
3.3 ARCHITECTURE

Designing a system for fake social media ID detection involves combining various techniques. Utilize machine learning models to analyze user behavior, image recognition for profile pictures, and natural language processing for text analysis. Implement anomaly detection algorithms to identify unusual patterns. Users can report suspicious accounts, and incorporate community-based reporting systems for enhanced accuracy. Regularly update the system to adapt to evolving fake ID tactics. Privacy considerations and ethical guidelines should be a priority throughout the design process.



3.4 USE CASE DIAGRAMS

In the use case diagram for a fake profile social media platform, the primary actors are Users, Administrators, and the System. Users can register, login, create fake profiles, search for other fake profiles, send friend requests, and post content on their profiles. Administrators have the authority to monitor and manage user activities, including identifying and taking action against fakeprofiles. The System itself encompasses processes such as user authentication, profile creation, content moderation, and friend request management. The interactions between these actors and use cases highlight the functionalities necessary for both users and administrators to engage with the platform while maintaining a balance between user freedom and system integrity. The diagram visually represents the relationships and dependencies between the various elements of the fake profile social media system, providing a comprehensive overview of its functionality.



CHAPTER 4

MODULE DESCRIPTION

REGISTRATION MODULE

Developing a registration module for a social media platform involves creating a system to authenticate users and ensure the validity of their profiles. Implementing security measures is crucial to prevent the creation of fake profiles. The registration process should include verification steps, such as email confirmation or phone number authentication, to ensure that users are genuine. Additionally, incorporating advanced technologies like facial recognition or CAPTCHA tests can add an extra layer of security. Regularly updating and monitoring the registration module helps in adapting to evolving tactics used by individuals attempting to create fake profiles. A well-designed registration system plays a pivotal role in maintaining the integrity and authenticity of a social media platform.

LOGIN MODULE

To counter fake profiles, consider incorporating user behavior analysis, anomaly detection, and IP address tracking. Regularly update security protocols to stay ahead of potential threats. Monitoring login activity and employing machine learning algorithms can help identify unusual patterns associated with fake profiles.

DETECTION MODULE

Implementing a robust detection module is crucial for identifying and mitigating fake social media profiles on a platform. Utilizing a combination of automated and manual methods enhances the effectiveness of the detection process.

1. Behavioral Analysis: Monitor user behavior patterns, such as posting frequency, content types, and interaction styles. Unusual or inconsistent behavior may indicate a fake profile.

2. Profile Completeness: Analyze the completeness of user profiles. Fake profiles often lack detailed information or use generic photos.

4. Content Analysis: Utilize natural language processing to analyze post content. Fake profiles may exhibit repetitive or inconsistent language patterns.

5. Cross-Platform Verification: Check for consistency across multiple social media platforms. Fake profiles often reuse content or have discrepancies in information.

6. User Reporting System: Implement a user-friendly reporting system to allow genuine users to flag suspicious profiles. Manual review can be conducted based on user reports.

7. Machine Learning Algorithms: Train machine learning models to identify patterns associated with fake profiles, considering factors like account creation patterns, posting behavior, and engagement metrics.

8. CAPTCHA and Human Verification: Integrate CAPTCHA or other human verification methods during critical interactions, like account creation or password recovery, to thwart automated bot activities.

10. Periodic Audits: Conduct regular audits of user accounts, especially those exhibiting suspicious behavior. This ensures ongoing vigilance against evolving tactics used by fake profiles.

By combining these techniques, a comprehensive detection module can significantly enhance the platform's ability to identify and address fake social media profiles. Regular updates and collaboration with cybersecurity experts can further strengthen the detection system.

CHAPTER 5

DESIGN AND DEVELOPMENT PROCESS

VS CODE

Visual Studio Code (VS Code) is a powerful code editor that can be used for various development situations. It's free, cross-platform, and open-source¹. It's not a .NET app, but it is written using Electron, a project from Github that makes it possible to develop desktop apps for Windows, macOS, and Linux using web technologies such as HTML, CSS, and JavaScript, or TypeScript¹.

VS Code is lightweight and should easily run on today's hardware. It requires a 1.6 GHz or faster processor and 1 GB of RAM². It is supported on the following platforms: Windows 10 and 11 (32-bit and 64-bit), macOS versions with Apple security update support, and Linux (Debian): Ubuntu Desktop 18.04, Debian 10²

PHP

PHP, which stands for Hypertext PreProcessor, is a widely used open-source and general-purpose server-side scripting language. It's primarily used in web development to create dynamic websites and applications¹.

When it comes to software specification, PHP can be used to define the behavior of the software you're developing. For instance, you can use PHP to specify how your software should interact with databases, handle user input, or display information on a webpage

HTML AND CSS

HTML (HyperText Markup Language) and CSS (Cascading Style Sheets) are fundamental technologies used in defining the structure and style of web pages¹. HTML provides the basic structure of sites, which is enhanced and modified by other technologies like CSS¹.

In the context of software specification, HTML and CSS can be used to create mockups or prototypes of software applications, particularly web applications. These prototypes can serve as a visual guide for how the software should look and function, and can be used to gather feedback from users or stakeholders before the actual development begins.

JAVA SCRIPT

JavaScript is a powerful scripting language that allows you to implement complex features on web pages¹. It's often used in web development to create dynamic websites and applications¹.

In terms of software specification, JavaScript can be used to define the behavior of the software you're developing. For instance, you can use JavaScript to specify how your software should interact with web pages, handle user input, or perform certain tasks

MySQL

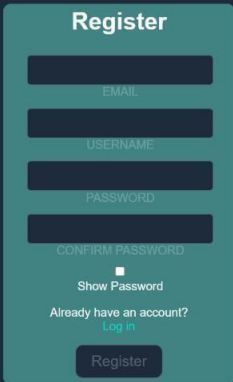
Leveraging MySQL for fake social media profile detection involves designing a comprehensive database schema to store user data and behavioral patterns. By implementing efficient queries, the system can analyze information for anomalies like unusual posting frequencies and inconsistent details. MySQL's capabilities also enable the creation of a reporting system, allowing users to flag suspicious profiles and submit detailed reports. The centralized database structure facilitates swift response and investigation. Integrating external data sources, such as IP geolocation services, enhances detection accuracy. Regular updates maintain the system's effectiveness in identifying emerging patterns associated with fake profiles, empowering users to actively contribute to the platform's security and authenticity..

CHAPTER 6

IMPLEMENTATION AND RESULTS

REGISTRATION PAGE

Developing a registration module for a social media platform involves creating a system to authenticate users and ensure the validity of their profiles.

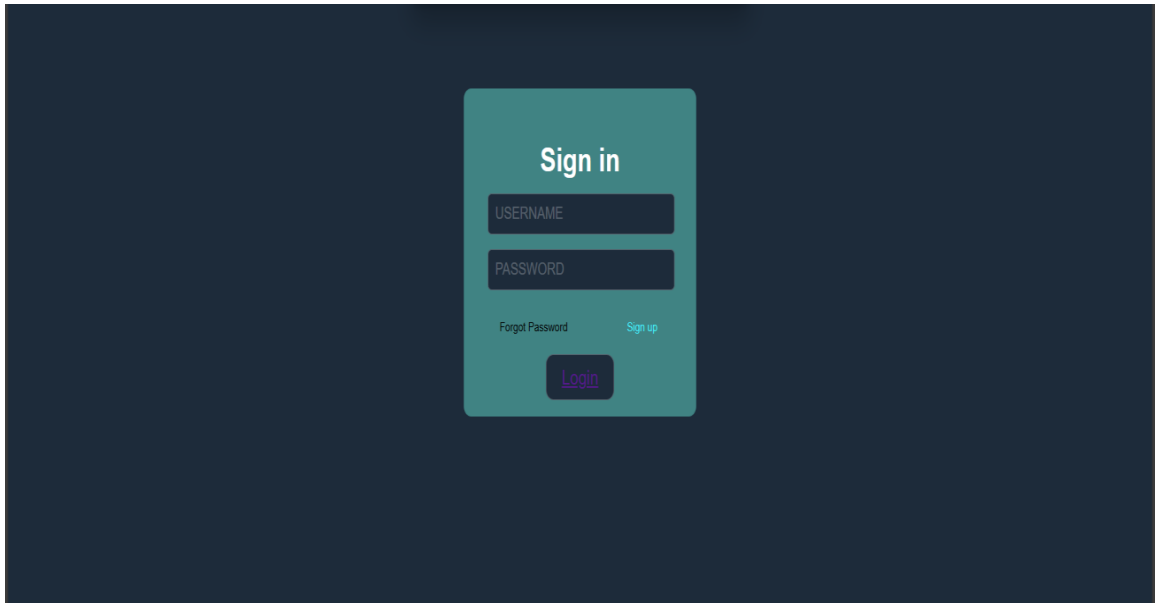


The image shows a registration form titled "Register" centered on a dark blue background. The form is a light teal color and contains the following elements:

- A title "Register" at the top.
- Four input fields with labels: "EMAIL", "USERNAME", "PASSWORD", and "CONFIRM PASSWORD".
- A "Show Password" toggle with a small square icon.
- A link "Log in" in red text.
- A "Register" button at the bottom.

LOGIN MODULE

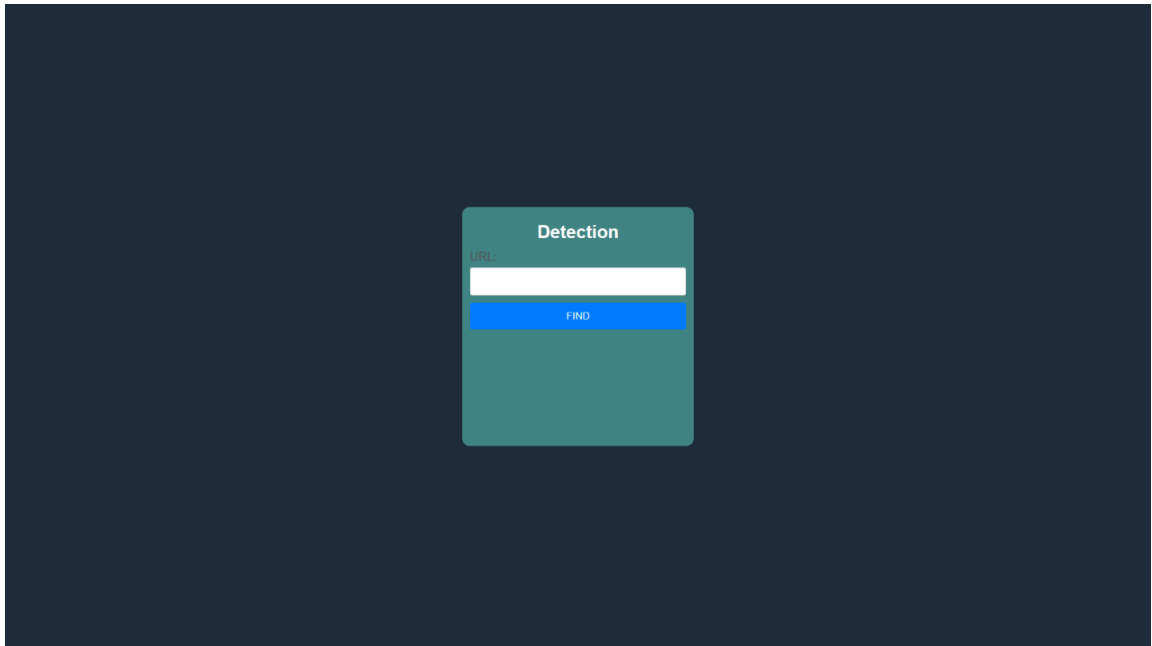
To counter fake profiles, consider incorporating user behavior analysis, anomaly detection, and IP address tracking.



The image shows a login module on a dark blue background. A teal-colored box is centered, containing the text "Sign in" at the top. Below this are two input fields: "USERNAME" and "PASSWORD". Under the "PASSWORD" field, there are two links: "Forgot Password" and "Sign up". At the bottom of the teal box is a button labeled "Login".

DETECTION MODULE

Implementing a robust detection module is crucial for identifying and mitigating fake social media profiles on a platform.



CHAPTER 7

CONCLUSION

The Fake Social Media Profile Detection and Reporting project stands as a testament to our commitment to fostering a secure, trustworthy, and resilient online environment for users globally. Through a continued collaborative effort between technology, user communities, and platform administrators, we aim to stay at the forefront of mitigating the impact of fake profiles and preserving the integrity of online discourse.

The structure of accounts in social media is analyzed and information about the user contained in them is highlighted. The main metrics of Facebook are considered and analyzed. Based on these metrics it is possible to define a fake account.

CHAPTER 8

FUTURE ENHANCEMENT

For future enhancements of the Fake Social Media Profile Detection and Reporting project, several avenues can be explored to bolster its effectiveness and user experience. Implementing machine learning algorithms could enhance the system's ability to autonomously identify evolving patterns of fake profiles, improving detection accuracy over time. To foster user engagement and collaboration, consider incorporating a community-driven feedback mechanism, allowing users to share insights and collectively refine the detection algorithms. Regular updates and staying abreast of technological advancements in the cybersecurity domain will be crucial for keeping the Fake Social Media Profile Detection and Reporting project at the forefront of combating emerging threats in the dynamic landscape of social media.

CHAPTER 9

APPENDICES

SIGN.html

```
<!DOCTYPE html>

<html lang="en">

<head>

  <meta charset="UTF-8">

  <meta http-equiv="X-UA-Compatible" content="IE=edge">

  <meta name="viewport" content="width=device-width, initial-scale=1.0">

  <title>Login Page</title>

  <link rel="stylesheet" href="style.css">

  <script src="app.js"></script>

  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-
awesome/5.13.0/css/all.min.css">

</head>

<body>

  <div class="container" method="post">

    <h1>Sign in</h1>

    <div class="inputFields">

      <input type="text" required="required">

      <span>Username</span>

    </div>

    <div class="inputFields">
```

```

        <input type="password" required="required">
        <span>Password</span>
    </div>

    <div class="links">
        <a href="#" class="forgotten" onclick="alert('Check your email for
confirmation!')">Forgot Password</a>
        <a href="register.html">Sign up</a> <br>
    </div>

    <div class="url">
        <button class="button1"><a href="valid.html">Login</a></button>
    </div>
</div>
</body>
</html>

```

REGISTRATION.html

```

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Register Forum</title>
    <link rel="stylesheet" href="style.css">
    <script src="app.js"></script>

```

```

</head>

<body>

  <div class="container2">

    <h1 class="secondH1">Register</h1>

    <div class="box">

      <input type="text" class="email" required="required">

      <span>Email</span>

      <input type="text" class="username" required="required">

      <span>Username</span>

      <input type="password" required="required" id="myInput1">

      <span>Password</span>

      <input type="password" class="confirmPassword" required="required"
id="myInput2">

      <span>Confirm Password</span>

      <input type="checkbox" onclick="myFunction()">Show Password

    </div>

    <div class="links2">

      <p>Already have an account?</p><a href="index.html">Log in</a>

    </div>

    <button class="button2"><a href="index.html">Register</a></button>

  </div>

</body>

```

</html>

DECETION.html

<html lang="en"><head>

 <meta charset="UTF-8">

 <meta name="viewport" content="width=device-width, initial-scale=1.0">

 <title>Valid</title>

 <link rel="stylesheet" href="style.css">

</head>

<body>

 <div class="container">

 <h2>Detection</h2>

 <form action="login.php" method="POST">

 <div style="margin: 10px 0; text-align: left;">

 <label for="URL" style="display: block; margin-bottom: 5px; color: #555;">URL:</label>

 <input type="text" id="URL" name="URL" required="" style="width: 100%; padding: 10px; border: 1px solid #ccc; border-radius: 3px;">

 </div>

 <div style="margin: 10px 0; text-align: left;">

 </div>

 <button type="submit" style="width: 100%; padding: 10px; background-color: #007BFF; color: #fff; border: none; border-radius: 3px; cursor: pointer;">FIND</button>

 </form>

```
</div>
</body></html>
```

CSS

```
* {
  margin: 0;
  padding: 0;
  box-sizing: border-box;
  font-family: "Poppins", sans-serif;
}

h1 {
  margin-top: 11%;
}

body { display: flex;
  justify-content: center; align-items: center; min-height: 100vh; flex-direction:
  column; gap: 30px;
  background-color: #1d2b3a;
}
```

```
.container {  
    text-align: center; color: white; width: 310px; height: 320px; position: relative;  
    background: rgb(64, 131, 131); padding: 20px 10px 10px; border-radius: 10px;  
}  
  
.name {  
    margin-bottom: 20px;  
}  
  
.links { display: flex;  
    justify-content: space-between;  
}  
  
.links a { margin: 10px 0;  
    font-size: 0.75em; color: #45f3ff; margin-top: 10%;
```

```

margin-left: 13%; text-decoration: none;
}

.links a:hover {color: black;
}

.inputFields { position: relative; width: 250px; margin-top: 5%;
margin-left: 7.5%;
}

.inputFields input {width: 100%; padding: 10px;
border: 1px solid rgba(255, 255, 255, 0.25); background: #1d2b3a;
border-radius: 5px; outline: none; color: #fff;
font-size: 1em;
}

.inputFields span {

```



```
position: absolute;left: 0;
padding: 10px; pointer-events: none;font-size: 1em;
color: rgba(255, 255, 255, 0.25);text-transform: uppercase; transition: 0.5s;
}
```

```
.inputFields input:valid ~ span,
.inputFields input:focus ~ span {color: #00dfc4;
transform: translateX(10px) translateY(-7px);font-size: 0.65em;
padding: 0 10px; background: #1d2b3a;
border-left: 1px solid #00dfc4; border-right: 1px solid #00dfc4;
}
```

```
.button1 {
border: 1px solid rgba(255, 255, 255, 0.25);padding: 10px 20px;
```

```
font-size: 20px;cursor: pointer;margin: 10px;
color: rgba(255, 255, 255, 0.25);position: relative;
overflow: hidden; border-radius: 10px; background: #1d2b3a;
}
.button1:hover{ background: #00dfc4;color: black;
}
.button1::before{ content: ""; position: absolute;left: 0;
width: 100%;
height: 0%;
z-index: -1; transition: 0.8s;
}
.button1:hover::before{height: 180%;
```

```
}  
  
.container2 {  
    text-align: center; color: white; width: 310px; height: 510px; position: relative;  
    background: rgb(64, 131, 131); padding: 20px 10px 10px; border-radius: 10px;  
}  
  
.box {  
    position: relative; width: 250px; margin-top: 5%;  
    margin-left: 7.5%;  
}  
  
.box input { width: 100%; padding: 10px;  
    border: 1px solid rgba(255, 255, 255, 0.25); background: #1d2b3a;  
    border-radius: 5px; outline: none;
```

```
color: #fff; font-size: 1em;
margin-top: 5%;
}

.box span{ position: relative;left: 0;
padding: 10px; pointer-events: none;font-size: 1em;
color: rgba(255, 255, 255, 0.25);text-transform: uppercase; transition: 0.5s;
}

.box input:valid ~ span,
.box input:focus ~ span {color: #00dfc4;
transform: translateX(10px) translateY(-7px);font-size: 0.65em;
padding: 0 10px; background: #1d2b3a;
border-left: 1px solid #00dfc4; border-right: 1px solid #00dfc4;
```

```
}
```

```
.button2 {
```

```
border: 1px solid rgba(255, 255, 255, 0.25);padding: 10px 20px;
```

```
font-size: 20px;cursor: pointer;margin: 10px;
```

```
color: rgba(255, 255, 255, 0.25);position: relative;
```

```
overflow: hidden; border-radius: 10px; background: #1d2b3a;margin-top: 5%;
```

```
}
```

```
.button2:hover{ background: #00dfc4;color: black;
```

```
}
```

```
.button2::before{ content: ""; position: absolute;left: 0;
```

```
width: 100%;  
height: 0%;  
z-index: -1; transition: 0.8s; background: #45f3ff;  
color: rgba(255, 255, 255, 0.25);  
}
```

```
.button2:hover::after{top: 0%;  
border-radius: 10px;  
}
```

```
.links2{  
margin-top: 6%;  
}
```

```
.links2 a{  
color: #00dfc4;  
text-decoration: none;  
}
```

```
.links2 a:hover {color: black;  
}
```

```
.secondH1{ margin-top: -5%;  
}  
  
.showPassword{ color: #00dfc4;  
}  
  
form i {  
    margin-left: -30px;cursor: pointer;  
}
```

REFERENCE

[1] Van Der Walt, E. and Eloff, J. (2018) Using Machine Learning to Detect Fake Identities: Bots vs Humans. IEEE Access, 6, 6540-6549.

<https://doi.org/10.1109/ACCESS.2018.2796018>

[2] Kudugunta, S. and Ferrara, E. (2018) Deep Neural Networks for Bot Detection. Information Sciences, 467, 312-322.

<https://doi.org/10.1016/j.ins.2018.08.019>

[3] Ramalingam, D. and Chinnaiah, V. (2018) Fake Profile Detection Techniques in Large-Scale Online Social Networks: A Comprehensive Review. Computers & Electrical Engineering, 65, 165-177.

<https://doi.org/10.1016/j.compeleceng.2017.05.020>

[4] Hajdu, G., Minoso, Y., Lopez, R., Acosta, M. and Elleithy, A. (2019) Use of Artificial Neural Networks to Identify Fake Profiles. 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, 3 May 2019, 1-4.

<https://doi.org/10.1109/LISAT.2019.8817330>

[5] Swe, M.M. and Myo, N.N. (2018) Fake Accounts Detection on Twitter Using Blacklist. 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), Singapore, 6-8 June 2018, 562-566.

<https://doi.org/10.1109/ICIS.2018.8466499>

[6] Wanda, P. and Jie, H.J. (2020) DeepProfile: Finding Fake Profile in Online Social Network Using Dynamic CNN. Journal of Information Security and Applications, 52, Article ID: 102465.

<https://doi.org/10.1016/j.jisa.2020.102465>

[7] Kodati, S., Reddy, K.P., Mekala, S., Murthy, P.S. and Reddy, P.C.S. (2021) Detection of Fake Profiles on Twitter Using Hybrid SVM Algorithm. E3S Web of Conferences, 309, Article No. 01046.

<https://doi.org/10.1051/e3sconf/202130901046>

[8] Meshram, E.P., Bhambulkar, R., Pokale, P., Kharbikar, K. and Awachat, A. (2021) Automatic Detection of Fake Profile Using Machine Learning on Instagram. *International Journal of Scientific Research in Science and Technology*, 8, 117-127.

<https://doi.org/10.32628/IJSRST218330>

[9] Chakraborty, P., Muzammel, C.S., Khatun, M., Islam, S.F. and Rahman, S. (2020) Automatic Student Attendance System Using Face Recognition. *International Journal of Engineering and Advanced Technology (IJEAT)*, 9, 93- 99.

<https://doi.org/10.35940/ijeat.B4207.029320>

[10] Sayeed, S., Sultana, F., Chakraborty, P. and Yousuf, M.A. (2021) Assessment of Eyeball Movement and Head Movement Detection Based on Reading. In: Bhattacharyya, S., Mršić, L., Brkljačić, M., Kureethara, J.V. and Koeppen, M., Eds., *Recent Trends in Signal and Image Processing*, Springer, Singapore, 95-103.

https://doi.org/10.1007/978-981-33-6966-5_10

[11] Chakraborty, P., Yousuf, M.A. and Rahman, S. (2021) Predicting Level of Visual Focus of Human's Attention Using Machine Learning Approaches. In: Shamim Kaiser, M., Bandyopadhyay, A., Mahmud, M. and Raym K., Eds., *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*, Springer, Singapore, 683-694.

https://doi.org/10.1007/978-981-33-4673-4_56

[12] Muzammel, C.S., Chakraborty, P., Akram, M.N., Ahammad, K. and Mohibullah, M. (2020) Zero-Shot Learning to Detect Object Instances from Unknown Image Sources. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 9, 988-991.

<https://doi.org/10.35940/ijitee.C8893.029420>

[13] Sultana, M., Ahmed, T., Chakraborty, P., Khatun, M., Hasan, M.R. and Uddin, M.S. (2020) Object Detection Using Template and Hog Feature Matching. *International Journal of Advanced Computer Science and Applications*, 11, 233-238.

<https://doi.org/10.14569/IJACSA.2020.0110730>

[14] Faruque, M.A., Rahman, S., Chakraborty, P., Choudhury, T., Um, J.S. and Singh, T.P. (2021) Ascertaining Polarity of Public Opinions on Bangladesh Cricket Using Machine Learning Techniques. *Spatial Information Research*, 30, 1-8.

<https://doi.org/10.1007/s41324-021-00403-8>

[15] Sarker, A., Chakraborty, P., Sha, S.S., Khatun, M., Hasan, M.R. and Banerjee, K. (2020) Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data. *Journal of Computer and Communications*, 8, 50-62.

<https://doi.org/10.4236/jcc.2020.87005>

[16] Ahammad, K., Shawon, J.A.B., Chakraborty, P., Islam, M.J. and Islam, S. (2021) Recognizing Bengali Sign Language Gestures for Digits in Real Time using Convolutional Neural Network. *International Journal of Computer Science and Information Security (IJCSIS)*, 19, 11-19.

[17] Sultana, M., Chakraborty, P. and Choudhury, T. (2022) Bengali Abstractive News Summarization Using Seq2Seq Learning with Attention. In: Tavares, J.M.R.S., Dutta, P., Dutta, S. and Samanta, D., Eds., *Cyber Intelligence and Information Retrieval*, Springer, Singapore, 279-289.

https://doi.org/10.1007/978-981-16-4284-5_24

[18] Ahmed, M., Chakraborty, P. and Choudhury, T. (2022) Bangla Document Categorization Using Deep RNN Model with Attention Mechanism. In: Tavares, J.M.R.S., Dutta, P., Dutta, S. and Samanta, D., Eds., *Cyber Intelligence and Information Retrieval*, Springer, Singapore, 137-147.

https://doi.org/10.1007/978-981-16-4284-5_13

[19] Reddy, S.D.P. (2019) Fake Profile Identification Using Machine Learning. *International Research Journal of Engineering and Technology (IRJET)*, 6, 1145-1150.

[20] Khaled, S., El-Tazi, N. and Mokhtar, H.M. (2018) Detecting Fake Accounts on Social Media. 2018 IEEE International Conference on Big Data (Big Data), Seattle, 10-13 December 2018, 3672-3681.

<https://doi.org/10.1109/BigData.2018.8621913>

[21] Elyusufi, Y. and Elyusufi, Z. (2019) Social Networks Fake Profiles Detection Using Machine Learning Algorithms. In: Ahmed, M.B., Boudhir, A.A., Santos, D., El Aroussi, M. and Karas, I.R., Eds., *Innovations in Smart Cities Applications Edition 3*, Springer, Cham, 30-40.

https://doi.org/10.1007/978-3-030-37629-1_3

[22] Joshi, U.D., Singh, A.P., Pahuja, T.R., Naval, S. and Singal, G. (2021) Fake Social Media Profile Detection. In: Srinivas, M., Sucharitha, G., Matta, A. and Chatterjee, P., Eds., *Machine Learning Algorithms and Applications*, Scrivener Publishing LLC, Beverly, MA, 193-209.

<https://doi.org/10.1002/9781119769262.ch11>

[23] Yuan, D., Miao, Y., Gong, N. Z., Yang, Z., Li, Q., Song, D., Wang, D. and Liang, X. (2019) Detecting Fake Accounts in Online Social Networks at the Time of Registrations. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London, 11-15 November 2019, 1423-1438.

<https://doi.org/10.1145/3319535.3363198>

[24] Roy, P.K. and Chahar, S. (2020) Fake Profile Detection on Social Networking Websites: A Comprehensive Review. *IEEE Transactions on Artificial Intelligence*, 1, 271-285.

<https://doi.org/10.1109/TAI.2021.3064901>