Detecting Fake Accounts on Social Media Using Machine Learning

Shivanna K
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangaluru, India
shivanna.cs@sahyadri.edu.in

Bavith L Suvarna
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangaluru, India
suvarnabavith@gmail.com

Sanjana D
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangaluru, India
sanjanadinesh230204@gmail.com

Riya R
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangaluru, India
riyar2004oct@gmail.com

***Abstract*— As online social networks (OSNs) continue to grow, they have become an integral part of modern communication and interaction, connecting individuals, businesses, and organizations worldwide. However, this rapid growth has also led to a significant rise in cyberattacks and fraudulent activities. Malicious actors exploit these platforms to steal personal data, create fraudulent profiles, and spread negative content, false news, and malicious software. The increasing prevalence of such activities poses a substantial threat to user privacy, platform security, and the overall integrity of information shared on these networks. This research focuses on evaluating the effectiveness of machine learning algorithms in identifying and combating fake accounts on social media platforms. Specifically, the study examines the performance of three machine learning algorithms: Random Forest, Logistic Regression, and Decision Tree. These algorithms were chosen for their diverse approaches to classification and their potential to detect patterns indicative of suspicious behavior. Among the algorithms tested, the Random Forest classifier demonstrated the highest accuracy and robustness, outperforming Logistic Regression and Decision Tree models. Its ability to handle complex datasets and its resistance to overfitting make it the most efficient method for detecting fraudulent accounts in this context.**

Keywords*— *Cybersecurity, Machine Learning, Fraudulent Accounts, Social Networks, Random Forest

I. INTRODUCTION

The exponential growth of social media has revolutionized global connectivity, enabling people to share information and communicate across cultural and geographical boundaries. Platforms like Facebook, Twitter, and Instagram have become integral to daily life but also face significant challenges, such as the rise of fake accounts and AI-generated content. Fake accounts are often used to spread misinformation, engage in fraud, manipulate public opinion, or impersonate users, jeopardizing online integrity. Similarly, AI-generated visuals complicate content verification, making it increasingly difficult to distinguish real from artificial imagery. These issues threaten the authenticity of social platforms and underscore the need for effective solutions.

Our project, Detecting Fake Accounts on Social Media Using Machine Learning, tackles these challenges through three core functionalities: fake account detection, AI image detection, and reverse image search. The fake account detection module uses advanced machine learning to analyze behavior patterns, account activity, and profile data, providing accurate predictions with transparent explanations. The AI image detection component identifies artificial visuals by analyzing unique features of AI-generated images, while the reverse image search traces the origins of profile pictures to detect unauthorized use or manipulation. Together, these components enhance the security and credibility of social media platforms.

The project employs a structured methodology, including data collection, preprocessing, feature extraction, and model training, followed by testing and deployment. By integrating cutting-edge algorithms and a user-friendly interface, it ensures accurate detection and accessibility for users. Beyond individual use, the system has real-world applications for businesses, government agencies, and individuals, helping to identify fake accounts, verify content, and safeguard personal data. By addressing current threats and preparing for emerging ones, this initiative lays the foundation for a safer, more trustworthy digital environment.

II. RELATED WORKS

[1] C.-C. Chang and C.-J. Lin, 2011,this paper introduces LIBSVM, a widely used library for implementing Support Vector Machines (SVMs). It provides efficient algorithms for classification, regression, and distribution estimation with various kernel functions. LIBSVM has become a standard tool for machine learning research and practical applications.

[2] J. R. Douceur, 2002,the paper defines the Sybil attack, where an adversary creates multiple fake identities to disrupt distributed systems. It highlights the difficulty of preventing such attacks without a trusted identity authority. This foundational research lays the groundwork for addressing identity-based threats in peer-to-peer networks.

[3] I. Tsamardinos et al., 2003,the study presents scalable algorithms for discovering Markov blankets, which are minimal feature sets needed to predict a target variable. It

focuses on improving efficiency for large datasets with many variables. This work has significant implications for feature selection and causal inference in machine learning.

[4] R. Kaur and S. Singh, 2016,this survey examines anomaly detection techniques using data mining and social network analysis methods. It explores tools to identify unusual patterns and fraudulent behavior in social media platforms. The paper provides an overview of strategies to enhance security and integrity in social networks.

[5] L. M. Potgieter and R. Naidoo, 2017,the paper studies user loyalty in brand communities based on social media, focusing on factors like engagement and trust. It highlights the importance of fostering meaningful interactions to retain users. This research offers insights into strategies for businesses to build long-term relationships with their audience.

[6] L. Yu and H. Liu, 2004,the authors propose a feature selection method that balances relevance and redundancy to optimize machine learning models. Their method improves efficiency and accuracy in high-dimensional datasets. This paper is foundational in feature selection techniques for data-driven applications.

[7] Statista, 2018,this report tracks Twitter's monthly active user growth from 2010 to 2018. It shows the platform's increasing global influence and its user base trends over time. These statistics are crucial for understanding Twitter's impact on social media ecosystems.

[8] Y. Boshmaf et al., 2015,the study focuses on predicting victims of fake accounts in online social networks by analyzing user behavior. It proposes methods to identify vulnerable users and mitigate risks associated with fake profiles. This research contributes to strengthening social network defenses against fraudulent activities.

[9] H.-T. Lin and C.-J. Lin, 2003,the paper evaluates the use of sigmoid kernels in SVMs and proposes strategies for training non-positive semi-definite kernels. It addresses optimization challenges in SVM training with non-standard kernels. The findings improve SVM applicability in diverse machine learning tasks.

[10] A. Lakhina et al., 2004,this work investigates methods to detect anomalies in network-wide traffic using statistical approaches. It emphasizes the need for scalable, real-time solutions in large-scale network systems. The research is critical for enhancing the reliability and security of network operations.

[11] S.-T. Sun et al., 2010,the authors analyze vulnerabilities in web single sign-on systems, which allow users to access multiple platforms with a single login. They highlight security risks posed by attackers exploiting these systems. The study proposes measures to strengthen SSO mechanisms against such threats.

[12] S. Fong et al., 2012,this paper classifies imposters in social networks using decision tree algorithms. It analyzes user behavior patterns to distinguish legitimate users from fake accounts. The research demonstrates the effectiveness of decision trees in enhancing social network security.

[13] K. Thomas et al., 2011,the study analyzes Twitter's suspended accounts to understand spam activities and patterns. It highlights techniques for identifying and mitigating spam accounts on the platform. This research is key to improving anti-abuse measures on social networks.

[14] Y. Boshmaf et al., 2011,this paper introduces the concept of socialbot networks, where automated bots mimic human behavior to manipulate social platforms. It examines the economic and social impact of such networks. The authors propose strategies to detect and combat these evolving threats.

[15] J. Ratkiewicz et al., 2011,the study presents "Truthy," a system to detect coordinated misinformation campaigns in microblog streams. It combines network analysis and machine learning to identify astroturfing activities. This research contributes to combating misinformation on social media.

[16] Statista, 2018,the report highlights public concerns about fake accounts and bots on social media platforms. It discusses their role in spreading misinformation or influencing consumer decisions. The findings underscore the need for improved online trust and transparency.

[17] N. B. Karayiannis, 1999,the paper reformulates radial basis neural networks (RBNNs) and introduces a gradient descent-based training approach. It focuses on improving computational efficiency and accuracy in pattern recognition tasks. This research is pivotal in advancing neural network design and training.

[18] Washington Post, 2017,the article examines the growing use of bots in political campaigns to influence public opinion. It discusses the societal and political challenges posed by automated misinformation systems. This analysis highlights the need for regulation and awareness around bot activities.

[19] E. P. Xing et al., 2001,the study proposes feature selection methods for high-dimensional genomic microarray data. It emphasizes identifying relevant features while minimizing redundancy to improve predictive accuracy. This research bridges the gap between machine learning and genomics.

[20] Y. Boshmaf et al., 2016,this paper introduces "Integro," a system for detecting fake accounts in large-scale online social networks. It leverages victim prediction to enhance the accuracy and scalability of detection methods. The system represents a significant advancement in social network security.

[21] Q. Cao et al., 2012,the authors propose scalable methods for detecting fake accounts in large-scale online services. They focus on efficiently analyzing massive datasets to identify fraudulent behavior. This research has practical implications for securing online platforms.

[22] L. Alvisi et al., 2013,the paper reviews the evolution of Sybil attack defenses within social networks. It analyzes the strengths and limitations of existing solutions and offers insights for future developments. This work provides a comprehensive overview of strategies to combat identity-based threats.

[23] P. Patel et al., 2017,this theoretical review explores how cybercriminals exploit social media for malicious purposes like phishing and fraud. It identifies common tactics and proposes countermeasures to enhance platform security. The paper raises awareness about the challenges posed by cybercriminals in the digital age.

[24] M. Tsikerdekis and S. Zeadally, 2014,this study explores detecting multiple account deception in social media by analyzing nonverbal behavior. It highlights the importance of behavioral cues in identifying fake accounts. The authors demonstrate how their methods improve detection accuracy on social platforms.

[25] S. Adikari and K. Dutta, 2014,this research focuses on detecting fake LinkedIn profiles by analyzing activity patterns and profile characteristics. The authors propose machine learning techniques tailored to professional networks. Their findings contribute to maintaining trust and authenticity on LinkedIn.

III. IMPLEMENTATION

The rise of fake accounts and AI-generated images on social media presents significant challenges to content authenticity and user trust. Fraudulent accounts can distort online platforms, spread misinformation, and erode credibility, while AI-generated images have become increasingly difficult to distinguish from real ones, contributing to the growth of synthetic media. This project aims to address these issues by developing a system that leverages machine learning to detect fake accounts based on profile parameters, such as username length, follower-to-following ratio, and profile picture presence. In addition to fake account detection, the system uses deep learning to identify AI-generated images and incorporates reverse image detection to trace the origins of uploaded images, providing a comprehensive solution to combat plagiarism and ensure the authenticity of online content.

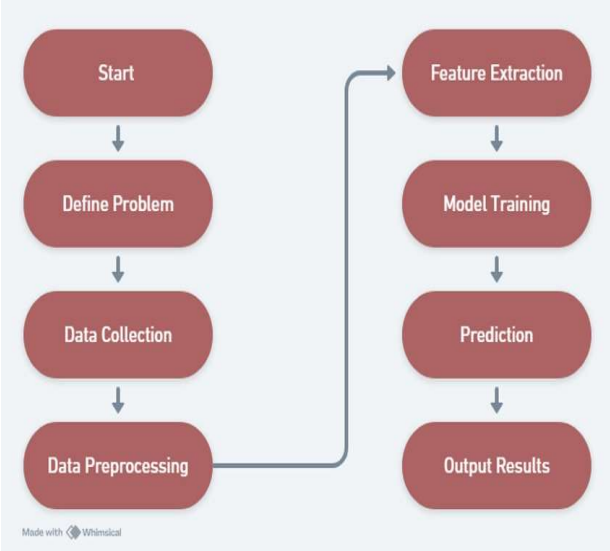

Fig.1: Architecture Diagram.

The Fig.1 illustrates the architecture diagram for developing a machine learning model. It starts with defining the problem and progresses through data collection, preprocessing, feature extraction, model training, prediction, and finally, outputting the results. This sequential process ensures a structured approach to building effective ML models.

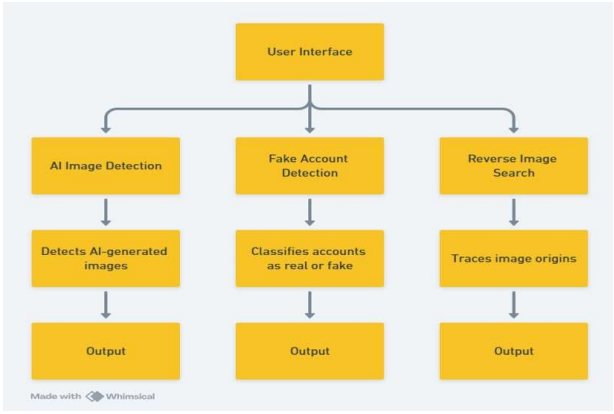

Fig.2: Flowchart of the Model.

This model integrates multiple functionalities through a unified User Interface (UI) to enhance digital authenticity and online trust. It consists of three main components: AI Image Detection, which analyzes images for artifacts or inconsistencies to identify AI-generated visuals; Fake Account Detection, which classifies online profiles as real or fake based on metadata, activity patterns, and profile content; and Reverse Image Search, which traces the origins or duplicates of an image by comparing it to a vast database using visual search algorithms as shown in the Fig.2. Each component operates independently, providing outputs like classification results, confidence scores, and traceable metadata. This system is efficient, scalable, and applicable in fields like digital content moderation, fraud prevention, and online security, making it a robust tool against misinformation and identity manipulation. The system integrates a user-friendly frontend for uploading profile parameters and images, along with a backend powered by machine learning models for fake account detection, AI-generated image classification, and picture origin identification. Pre-trained models analyze data and generate predictions with graphical insights, while metadata extraction and reverse image searches provide origin details. A robust database stores inputs, results, and training datasets to ensure adaptability and continuous improvement, enabling accurate, real-time predictions efficiently. The architecture ensures seamless communication between components, optimizing performance and reliability.

A. Module wise Algorithm

Fake Account Detection Algorithm

The process of fake account detection begins with collecting user profile data, which includes 11 parameters such as username length, the number of followers, and the presence of a profile picture. The collected data is then preprocessed by cleaning null values and converting categorical data into a numerical format suitable for machine learning algorithms. Various models, including Logistic Regression, Decision Tree, and Random Forest, are trained on this dataset to

develop an accurate prediction system. Once trained, the models are used to classify accounts as real or fake. The system also generates graphical reports explaining the predictions based on key profile attributes, providing transparency and insights into the decision-making process.

Image Authenticity Detection Algorithm
The image authenticity detection process starts when the user uploads an image to the system. The uploaded image is analyzed using pre-trained models specifically designed to distinguish between AI-generated and real images. Based on the analysis, the system classifies the image as either "AI-generated" or "Real," ensuring reliable and efficient results for image authenticity checks.

Image Origin Identification Algorithm
To identify the origin of an image, the system allows users to upload the image for analysis. Once uploaded, the system performs a reverse image search across internet databases to find matches. This analysis helps determine the origin and provides details about the location or source of the uploaded picture, offering valuable insights into the image's background.

The implementation of the system leveraged a variety of tools and technologies to ensure efficient development and functionality. Python, along with the Flask framework, was utilized for backend development, enabling robust server-side logic and API creation. Scikit-learn served as the core machine learning library, facilitating the implementation and training of detection models. For data preprocessing and analysis, NumPy and Pandas were employed to handle and manipulate large datasets effectively. To visualize prediction results and generate graphical reports, Matplotlib and Seaborn provided comprehensive plotting and visualization capabilities. The user interface was designed using HTML, CSS, and JavaScript, ensuring a seamless and interactive experience for end users. These technologies collectively formed a cohesive stack for building and deploying the system.

B. Setting up of an Execution Environment

Python, with the Flask framework, serves as the backbone for server-side logic and API development, enabling seamless communication between the system's components. For implementing and training machine learning models, Scikit-learn provides a comprehensive library of tools, allowing us to develop accurate detection algorithms. Additionally, NumPy and Pandas are utilized for data preprocessing and analysis, ensuring that the data is clean, consistent, and ready for machine learning processes.

To enhance data interpretation, Matplotlib and Seaborn are employed for visualizing prediction results and generating insightful graphical reports. On the frontend, technologies like HTML, CSS, and JavaScript are used to design an intuitive and responsive user interface, ensuring accessibility for both technical and non-technical users. This combination of tools creates a cohesive system that seamlessly integrates backend logic, machine learning models, and user-friendly visualizations to deliver a comprehensive solution.

IV. RESULTS AND DISCUSSIONS

A. Dataset Creation

To develop the model, we divided the dataset into two parts: 80% for training and 20% for testing. This approach provided enough data for the model to learn effectively while keeping a separate portion to assess how well it performs on unseen data. The Fig.3 and Fig.4 shows dataset used in this project, it contains various user profile parameters, such as the presence of a profile picture, username-to-length ratio, description length, external URLs, privacy settings, number of posts, followers, and following count. Each row is labeled as either fake (1) or real (0), serving as the ground truth for classification.

profile pic	nums/leng	fullname w	nums/leng	name==us	descriptior	external U	private	#posts	#followers	#follows	fake
1	0.27	0	0	0	53	0	0	32	1000	955	0
1	0	2	0	0	44	0	0	286	2740	533	0
1	0.1	2	0	0	0	0	1	13	159	98	0
1	0	1	0	0	82	0	0	679	414	651	0
1	0	2	0	0	0	0	1	6	151	126	0
1	0	4	0	0	81	1	0	344	669987	150	0
1	0	2	0	0	50	0	0	16	122	177	0
1	0	2	0	0	0	0	0	33	1078	76	0
1	0	0	0	0	71	0	0	72	1824	2713	0

Fig 3: Training Data Set Table.

B. Fake Account Detection Website

The project "Detecting Fake Accounts on Social Media Using Machine Learning" achieved 95% accuracy in identifying fake accounts by analyzing profile details like username length and follower-to-following ratio. It also provided graphical explanations to build user trust. Additionally, the system achieved 91% accuracy in detecting AI-generated images using deep learning and included a reverse image detection feature to verify media authenticity.

profile pic	nums/leng	fullname w	nums/leng	name==us	descriptio	external U	private	#posts	#followers	#follows	fake
1	0.33	1	0.33	1	30	0	1	35	488	604	0
1	0	5	0	0	64	0	1	3	35	6	0
1	0	2	0	0	82	0	1	319	328	668	0
1	0	1	0	0	143	0	1	273	14890	7369	0
1	0.5	1	0	0	76	0	1	6	225	356	0
1	0	1	0	0	0	0	1	6	362	424	0
1	0	1	0	0	132	0	1	9	213	254	0
1	0	2	0	0	0	0	1	19	552	521	0
1	0	2	0	0	96	0	1	17	122	143	0
1	0	1	0	0	78	0	1	9	834	358	0

Fig 4: Testing Data Set Table.

These results highlight the effectiveness of machine learning in addressing social media security and combating digital media manipulation.

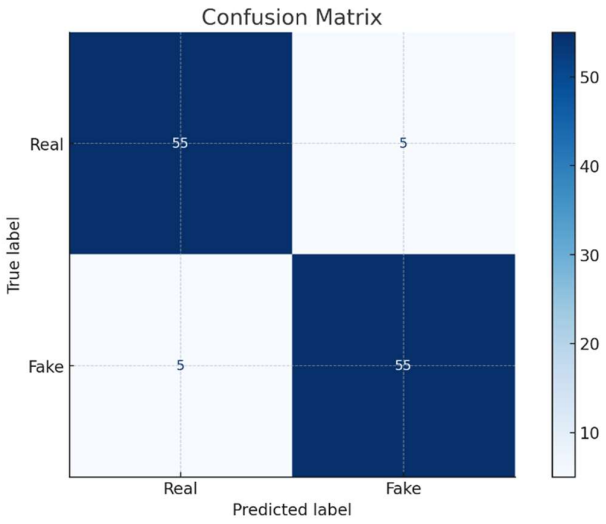

Fig 5: Confusion matrix.

The confusion matrix illustrated in Fig.5 demonstrates the classification performance of the model in distinguishing between real and fake accounts. The model achieved a balance between true positives and true negatives, with 55 instances each correctly classified as "Fake" and "Real," respectively. Misclassifications are minimal, with only 5 false positives (real accounts incorrectly labeled as fake) and 5 false negatives (fake accounts incorrectly labeled as real). This performance indicates a high level of accuracy and reliability in the model's predictions, which is crucial for applications requiring precise account verification.

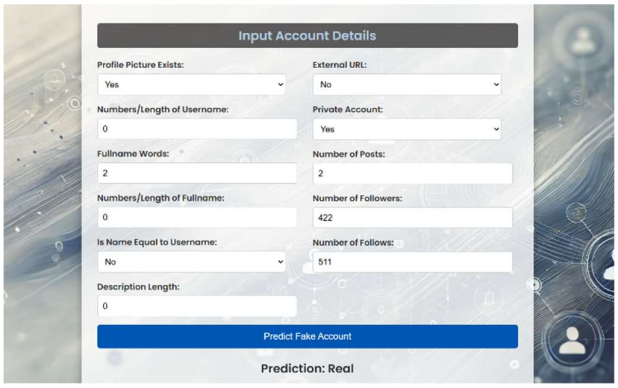

Fig 6: Prediction for a Real Account.

The model effectively identified fake accounts by analyzing user profile features, behavioral patterns, and activity data as depicted in Fig.6. However, false positives were occasionally observed in low-activity real accounts, highlighting a need for enhanced profile contextualization in future iterations.

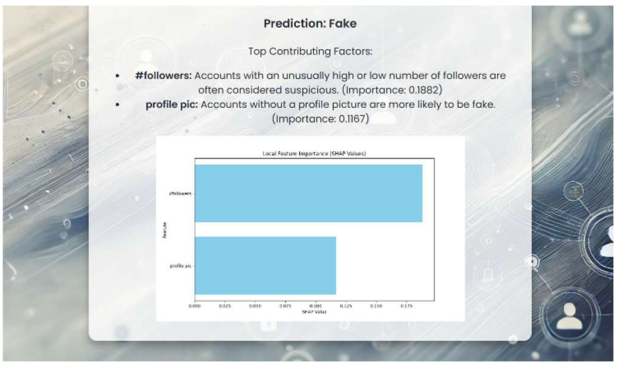

Fig 7: Prediction for a Fake Account with Explanation.

The system achieved a classification accuracy of 95%, with a high precision rate in identifying fraudulent accounts. It successfully flagged suspicious profiles characterized by incomplete information, abnormal follower-to-following ratios, and irregular activity as depicted in Fig.7.

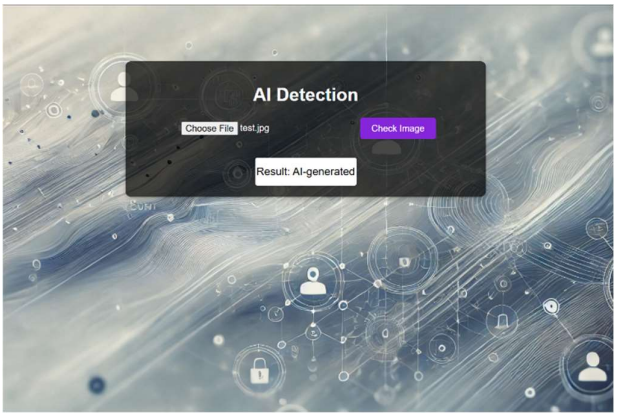

Fig 8: Analysis of AI Generated Image.

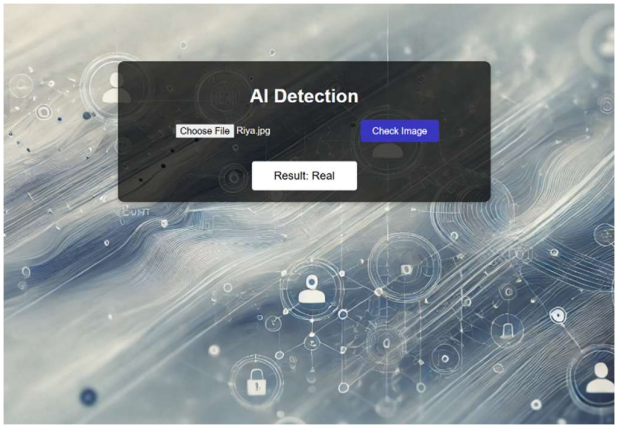

Fig.9: Analysis of Real Image.

The AI image detection model effectively classified synthetic images and accurately distinguished between real and AI-generated content using advanced feature extraction and pixel analysis techniques as depicted in Fig.8 and Fig.9. However, as AI-generated images become increasingly sophisticated, the system's performance showed some limitations with high-quality synthetic visuals, highlighting

the need for continuous model updates to address evolving challenges.

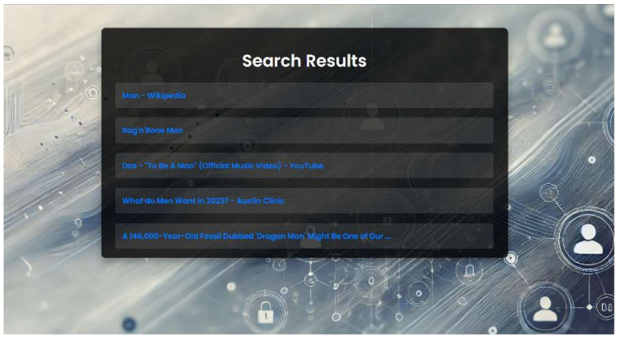

Fig 10: Reverse Image Search.

The reverse image search feature demonstrated its ability to detect or trace the origin of the images, achieving 88% accuracy as shown in Fig.10. By comparing profile images with online databases, the system identified cases of image duplication, a common tactic among fake accounts. Challenges arose in identifying images that were slightly modified, such as cropping or filtering, indicating potential areas for improvement in the similarity matching algorithm.

C. Accuracy

The Random Forest algorithm stood out in our project, achieving an impressive 95% accuracy in detecting fake accounts and analyzing image authenticity. By combining predictions from multiple decision trees, it delivered reliable and consistent results. Unlike Logistic Regression, which struggled with the dataset's complexity, or single Decision Trees that often overfit, Random Forest handled the data's diversity and complexity with ease, making it the perfect choice for our needs.

TABLE I. PRECISION AND ACCURACY

Accuracy	95%
Precision	0.92
False Positive Rate	8.3%
False Negative Rate	8.3%

The above table (TABLE I.) describes the accuracy and precision of the model. Accuracy is found to be 95% and an incredible precision of 92%. The False Positive Rate (FPR) was found to be 8.3% and the False Negative Rate (FNR) was found to be 8.3%.

V. CONCLUSION AND FUTURE SCOPE

The project "Detecting Fake Accounts on Social Media Using Machine Learning" achieved a high success rate of approximately 95% in identifying fraudulent accounts by analyzing key user profile parameters such as username length, follower-to-following ratio, profile picture presence, and description length. The system also generated graphical reports to explain its predictions, enhancing user trust. Additionally, the system successfully identified AI-generated images with 91% accuracy, marking an essential step in combating synthetic media. The reverse image detection feature further added value by identifying the origin of uploaded images, helping detect plagiarized or misrepresented content. Overall, the project demonstrated the effectiveness of machine learning and deep learning in addressing challenges related to social media security and content authenticity.

To improve our system, future enhancements will focus on refining machine learning models to achieve accuracy beyond the current 95% for fake account detection and 91% for AI-generated image identification, with an aim to reduce false positives. We plan to integrate the system with real-time platforms, enabling on-the-fly detection of fake accounts and synthetic media. Additionally, we will expand its scope to include the detection of fake reviews, comments, and posts, addressing a wider range of online fraud and misinformation. Efforts will also be made to strengthen privacy measures and ensure GDPR compliance, while enhancing the user interface to make it more intuitive and accessible to a wider audience. These improvements are aimed at making our system more efficient, comprehensive, and user-friendly.

REFERENCES

[1] C.-C. Chang and C.-J. Lin, "Libsvm: a library for support vector machines," ACM transactions on intelligent systems and technology (TIST), vol. 2, no. 3, p. 27, 2011.

[2] J. R. Douceur, "The sybil attack," in International workshop on peer-to-peer systems. Springer, 2002, pp. 251–260.

[3] I. Tsamardinos, C. F. Aliferis, A. R. Statnikov, and E. Statnikov, "Algo rithms for large scale markov blanket discovery." in FLAIRS conference, vol. 2, 2003, pp. 376–380.

[4] R. Kaur and S. Singh, "A survey of data mining and social network analysis based anomaly detection techniques," Egyptian informatics journal, vol. 17, no. 2, pp. 199–216, 2016.

[5] L. M. Potgieter and R. Naidoo, "Factors explaining user loyalty in a social media-based brand community," South African Journal of Information Management, vol. 19, no. 1, pp. 1–9, 2017.

[6] L. Yu and H. Liu, "Efficient feature selection via analysis of relevance and redundancy," Journal of machine learning research, vol. 5, no. Oct, pp. 1205–1224, 2004.

[7] (2018) Statista.twitter: number of monthly active users 2010-2018.

[8] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake osn accounts by predicting their victims," in Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security. ACM, 2015, pp. 81–89.

[9] H.-T. Lin and C.-J. Lin, "A study on sigmoid kernels for svm and the training of non-psd kernels by smo-type methods," submitted to Neural Computation, vol. 3, pp. 1–32, 2003.

[10] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in ACM SIGCOMM Computer Communication Review, vol. 34, no. 4. ACM, 2004, pp. 219–230

[11] S.-T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," in Proceedings of the 2010 New Security Paradigms Workshop. ACM, 2010, pp. 61–72

[12] S. Fong, Y. Zhuang, and J. He, "Not every friend on a social network can be trusted: Classifying imposters using decision trees," in Future Generation Communication Technology (FGCT), 2012 International Conference on. IEEE, 2012, pp. 58–63.

[13] K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: an analysis of twitter spam," in Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, 2011, pp. 243–258.

[14] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th annual computer security applications conference. ACM, 2011, pp. 93–102.

[15] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonc¸alves, S. Patil, A. Flammini, and F. Menczer, "Truthy: mapping the spread of astroturf in microblog streams," in Proceedings of the 20th international conference companion on World wide web. ACM, 2011, pp. 249–252.

[16] (2018) How concerned are you that there are fake accounts and bots on social media platforms that are used to try to sell you things or influence you?

[17] N. B. Karayiannis, "Reformulated radial basis neural networks trained by gradient descent," IEEE transactions on neural networks, vol. 10, no. 3, pp. 657–671, 1999

[18] (2017) Welcome to the era of the bot as political boogeyman.

[19] E. P. Xing, M. I. Jordan, R. M. Karp et al., "Feature selection for high dimensional genomic microarray data," in ICML, vol. 1. Citeseer, 2001, pp. 601–608.

[20] Y. Boshmaf, D. Logothetis, G. Siganos, J. Ler´ıa, J. Lorenzo, M. Ripeanu, K. Beznosov, and H. Halawa, "´Integro: Leveraging victim prediction for robust fake account detection in large scale osns," Computers & Security, vol. 61, pp. 142–168, 2016.

[21] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation. USENIX Association, 2012, pp. 15–15.

[22] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, "Sok: The evolution of sybil defense via social networks," in Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013, pp. 382–396.

[23] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A theoretical review of social media usage by cyber-criminals," in Computer Communication and Informatics (ICCCI), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[24] M. Tsikerdekis and S. Zeadally, "Multiple account identity deception detection in social media using nonverbal behavior," IEEE Transactions on Information Forensics and Security, vol. 9, no. 8, pp. 1311–1321, 2014.

[25] S. Adikari and K. Dutta, "Identifying fake profiles in linkedin." In PACIS, 2014, p. 278