iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** III **Month of publication:** March 2024

DOI: https://doi.org/10.22214/ijraset.2024.59275

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

Social Net Secure using Natural Language Processing and Machine Learning

Ms .M. Kamala[1], G. Vinayaswi Reddy[2], D. Honey Kezia[3], S. Yashwant[4]
[1]*Assistant Professor,* [2, 3, 4]*B.Tech, Department of Computer Science Engineering*

Abstract: ***In our contemporary era, social networking platforms have seamlessly integrated into the daily lives of the majority of individuals. With each passing day, a multitude of users create profiles on these platforms, fostering connections with others irrespective of geographical barriers or time constraints. While these platforms offer invaluable benefits to users, they also present inherent security challenges, particularly concerning the safeguarding of users' personal data. Addressing the risks associated with social networking platforms necessitates a systematic analysis of user profiles to discern potential threats. Through classification, we aim to distinguish between authentic and fraudulent profiles within these networks. Although various classification methods exist for detecting fake profiles, achieving optimal precision rates remains a formidable task. To enhance the precision rate of fake profile detection within social systems, this paper proposes the utilization of advanced Machine Learning (ML) and Natural Language Processing (NLP) techniques. Leveraging algorithms such as Support Vector Machine (SVM) and Naïve Bayes, we endeavor to refine the accuracy of identifying fraudulent profiles.***
Note: Machine Learning, Natural Language Processing.

I. INTRODUCTION

In today's digital era, social networking has evolved into a ubiquitous pastime on the internet, captivating millions of users who collectively invest billions of minutes in these services. Online Social Network (OSN) platforms span a wide spectrum, ranging from interaction-based platforms like Facebook and MySpace to information dissemination-centric platforms such as Twitter or Google Buzz, as well as social interaction features integrated into display systems like Flash.

However, amidst the popularity of social networking, enhancing security and safeguarding OSN privacy remains a significant challenge. When individuals engage with social networks, they inevitably share varying degrees of personal information, making them susceptible to various forms of attacks, with identity theft being one of the most concerning. Identity theft occurs when someone exploits another person's information for personal gain or malicious purposes.

In recent years, online identity theft has become a prevalent issue, affecting millions of individuals worldwide. Victims of identity theft may endure various consequences, including financial loss, legal troubles, reputational damage, and strained relationships with peers and loved ones. Unfortunately, the majority of SN platforms lack robust privacy and security measures, often defaulting to minimal privacy settings, thereby becoming fertile ground for fraud and abuse.

Social networking services have facilitated identity theft and impersonation attacks, attracting both sophisticated and naive attackers. Moreover, users are required to provide substantial personal information when creating accounts on these platforms, increasing the risk of devastating losses if accounts are compromised.

Profile information on online networks can be classified as either static or dynamic. Static information pertains to details provided by users during profile creation, while dynamic information refers to user interactions within the network. While much research focuses on static and dynamic data, this approach may overlook aspects of social networks where inactive profiles are prevalent, and dynamic profiles remain obscured.

Numerous methods have been proposed to detect fake identities and malicious content on online social networks, each with its own strengths and limitations. Issues such as privacy concerns, online bullying, abuse, and trolling are often exploited by fraudulent profiles on social networking sites. False profiles, characterized by fictitious credentials, engage in malicious activities that disrupt the social network experience for genuine users.

To address these challenges, platforms like Facebook employ security systems such as the Facebook Immune System (FIS) to protect user credentials from spamming and phishing attempts. Nonetheless, the battle to safeguard user privacy and security in the realm of social networking persists as a complex and ongoing endeavor.

Issues such as privacy, online bullying, abuse, trolling, and various others plague social networking platforms, often exploited by fraudulent profiles. False profiles, characterized by fabricated credentials, are prevalent on these platforms and engage in malicious activities that disrupt the online community.

These fraudulent profiles serve various purposes, including social engineering, online impersonation, defamation of individuals, and promotion or advocacy for specific causes or groups. Facebook, recognizing the severity of these issues, has implemented its own security measures to protect user credentials from threats like spamming and phishing. This security system, known as the Facebook Immune System (FIS), works tirelessly to safeguard user privacy and maintain the integrity of the platform.

II. LITERATURE REVIEW

The research conducted by Chai et al. presents a compelling case for the adoption of natural language processing and human-computer interaction in improving user experience. Despite utilizing conventional systems in these fields, the results garnered from user testing are remarkable.

In comparing their model approach with a conventional menu-driven method, they found that users, particularly novices, strongly prefer the natural language dialogue-based approach. Further, the study revealed that in an ecommerce setting, simplicity in interaction management outweighs the ability to handle complex natural language queries. To ensure easy access to information on ecommerce websites, a combination of natural language dialogue-based navigation and menu-driven navigation should be intelligently integrated to cater to users' diverse needs. Recently, the researchers have made significant advancements in their approach, incorporating enhancements in language processing, dialogue management, and information retrieval. They believe that natural language interaction offers effective personalized solutions compared to traditional menu-driven or search-based interfaces on websites

LinkedIn is widely popular among professionals in various industries. However, with the rapid expansion of social networks, there is an increasing risk of misuse for fraudulent and illegal activities. The creation of fake profiles poses a significant challenge, as distinguishing them without thorough research is difficult. Existing solutions primarily focus on analyzing the characteristics and social connections of users' profiles. However, LinkedIn's strict privacy policies limit the availability of publicly accessible profile information, rendering these methods ineffective. To address this issue, specific research is needed to develop methods for identifying fake profiles on LinkedIn.

Shalind Adikar and Koushik conducted research to identify the essential profile information necessary for detecting fake profiles on LinkedIn. They also determined the appropriate data mining techniques for this task. This focused approach aims to overcome the limitations posed by LinkedIn's privacy policies and improve the accuracy of fake profile detection on the platform..

Halimetal proposed a novel approach for spatio-temporal mining on social networks to identify circles of users involved in malicious activities through semantic analysis. They compared the results obtained from spatio-temporal co-occurrence with those derived from the original network ties, as the networks generated by spatio-temporal co-occurrence closely resembled genuine networks. By setting the threshold value appropriately, they selected a number of nodes, or actors, to achieve a clearer picture. Their findings indicated that Semantic Ordering was highly effective in detecting malicious content when the feature set was well-chosen. However, one limitation of this approach is how users select their feature set and its richness. If the feature set is too small, much of the malicious content may go undetected. Conversely, a larger feature set improves performance.

III. FRAMEWORK

A. Overview of the Proposed System

On this paper we included a ML common and dialect handling framework to watch the wrong profiles on social media and we are including the support vector machine classifier in and naïve bayes algorithm in additional to the discovery rate of the untrue profiles.

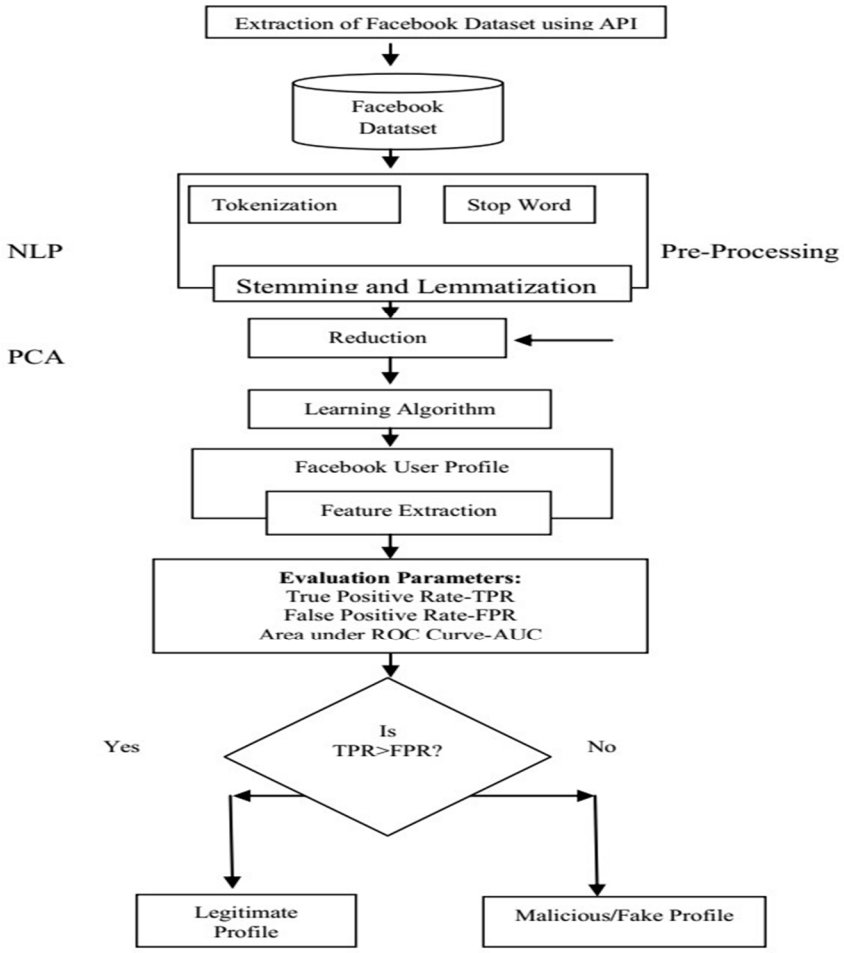


Figure 1. Working Method for Proposed Framework

The displayed handle utilized Facebook profile to take note untrue profiles. The working strategy of the proposed strategy incorporates three foremost stages:

Natural language Pre-processing ; Eigenanalysis; Learning Calculations

B. Natural Language Pre-Processing

Content preprocessing plays a fundamental role in any Natural Language Processing (NLP) strategy, offering several significant advantages:

1) Reduction of data size:

- Stop words account for approximately 20-30% of the total word count in a given text, leading to a considerable decrease in the overall size of the text data.
- Stemming can further reduce the data size by as much as forty to fifty percent.

2) Enhancement of productivity and effectiveness in Information Retrieval (IR) strategies:

- Elimination of stop words is essential as they do not contribute to meaningful content and may confuse the retrieval system.
- Stemming is valuable for matching similar words in a text document, thus improving the effectiveness of IR systems.

➢ Lexical Analysis: Lexical Analysis is the process of segmenting a stream of text into individual elements such as words, phrases, symbols, or other meaningful components known as tokens. Its purpose lies in the analysis of these elements within a sentence. The resulting list of tokens serves as input for further processing, including parsing or text mining tasks. Tokenization finds utility in both linguistics, where it serves as a form of text segmentation, and in computer science, where it constitutes a component of lexical analysis.

Text data initially consists of a sequence of characters. However, most methods in information retrieval require words from the dataset. Consequently, the need for tokenization arises. Although text is already stored in machine-readable codes, certain issues remain unresolved, such as the presence of punctuation marks. Various characters like brackets and hyphens also necessitate processing during tokenization.

- Stop word filtering: Stop words are commonly occurring words such as 'and', 'are', 'this', etc., that do not contribute significantly to the classification of documents. Therefore, they are typically removed from text data. However, compiling a comprehensive list of stop words can be challenging and may vary between different sources of text. Despite this challenge, removing stop words is beneficial as it reduces the volume of text data and improves processing efficiency. Every text document contains these non-essential words, which are irrelevant for content mining applications.

3) Morphological analysis: The purpose of Morphological analysis is for both stemming and lemmatization to reduce inflectional forms and derivationally related variations of a word to a standardized base form. Stemming typically involves a heuristic process of truncating word endings in the hope of achieving this objective accurately most of the time, often including the removal of derivational affixes. On the other hand, lemmatization refers to a more precise approach using a dictionary and morphological analysis of words, aiming to remove inflectional endings only and return the base or dictionary form of a word, known as the lemma.

4) Eigenanalysis

The purpose of eigenanalysis is to extract essential insights from data tables and represent them as a set of orthogonal components known as principal components. This technique aims to capture the fundamental structure of the data and assess the similarity between observations and factors represented as components in maps.

5) Learning Algorithm

In this framework we are utilizing two machine learning calculations named as Support Vector Machine (SVM) and naïve Bayes calculations.

C. Support Vector Machine (SVM)

The Support Vector Machine (SVM) is a powerful algorithm employed for data classification by identifying a hyperplane that effectively separates data points of different classes. The essence of SVM lies in locating this hyperplane with the maximum margin, providing the best possible distinction between the two classes. Essentially, SVM classifies data by identifying the unique hyperplane that cleanly separates all data points of one category from those of the other.

Central to SVM's operation are the support vectors, which are data points closest to the hyperplane. These support vectors essentially define the position and orientation of the hyperplane. By focusing on these critical data points, SVM ensures robust classification, even in complex datasets where classes might not be linearly separable.In essence, SVM excels in finding the optimal decision boundary between classes, ensuring effective classification even in scenarios where classes might overlap or be non-linearly separable.

D. Naïve Bayes

The Naive Bayes algorithm is renowned for its ability to ascertain the likelihood of an object, endowed with certain characteristics, belonging to a distinct category or group. Essentially, it serves as a probabilistic classifier. Termed "naive," the algorithm operates under the assumption that each feature's occurrence is independent of others—a characteristic that underlies its simplicity and efficiency. For instance, consider the task of identifying false profiles based on attributes such as timing, publication dates, content, language, and geographical location. Despite potential interdependencies among these factors, the Naive Bayes algorithm treats each property as contributing independently to the likelihood of a profile being fake.

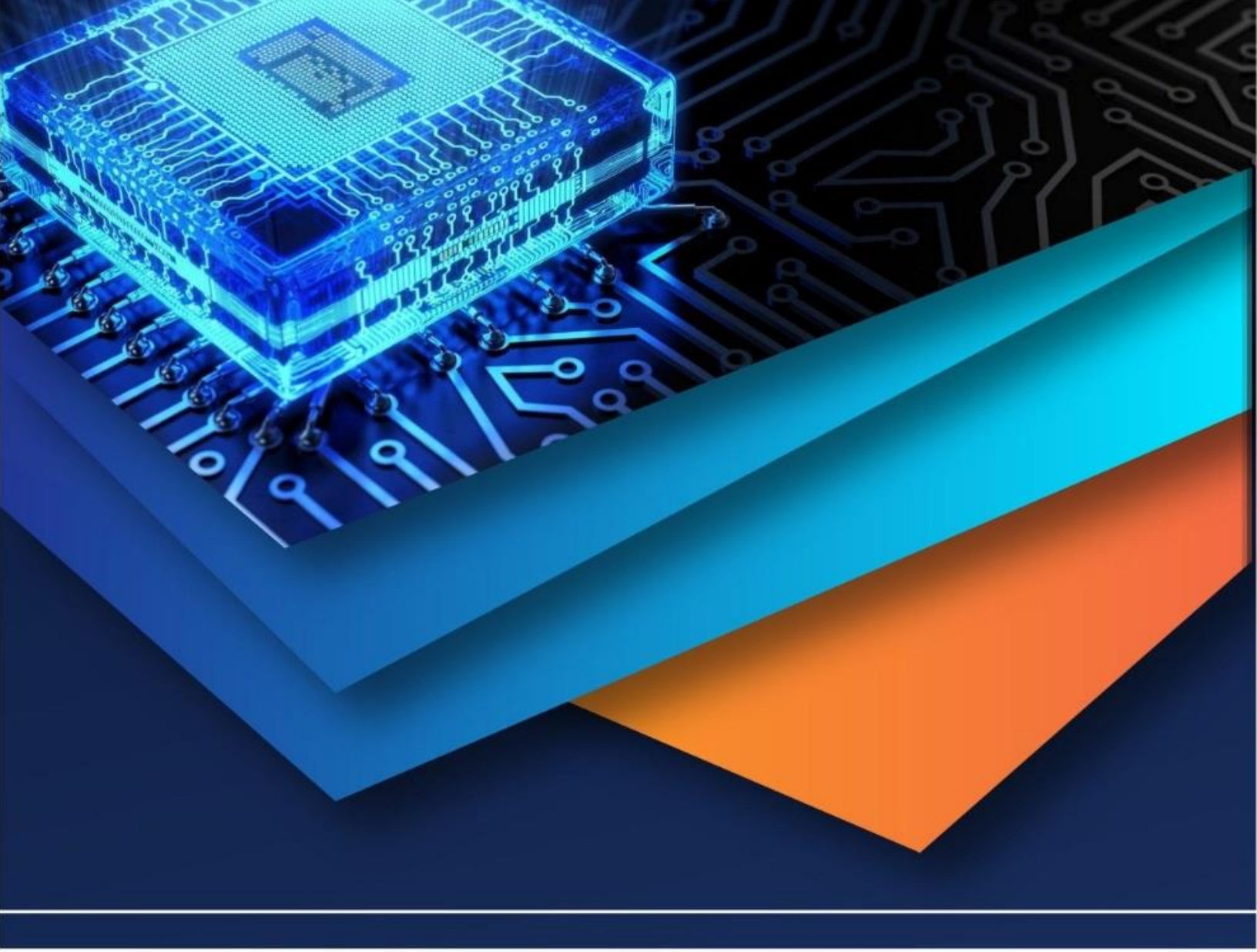
IV. CONCLUSION

In our research, we introduced a novel approach that combines machine learning algorithms with natural language processing (NLP) techniques to tackle the issue of identifying fake profiles on social networking platforms. Specifically, our focus was on analyzing Facebook data to discern fraudulent profiles. We employed NLP pre-processing methods to meticulously examine the dataset, followed by the application of machine learning algorithms such as Support Vector Machine (SVM) and Naïve Bayes for profile classification.

Through the integration of these sophisticated methodologies, we achieved notable advancements in the accuracy of fake profile detection. Our study demonstrates that leveraging SVM and Naïve Bayes algorithms significantly enhances the precision of identifying fake profiles within social networks.

REFERENCES

[1] Social systems based on topology peculiarities." Human Diary 1(1): 26-39.Günther, F. and S. Fritsch (2010). IEEE Conference on Machine Learning and IOT,Issue Date:12.May.2022 "neuralnet: Preparing of neural systems." The R Diary 2(1): 30-38
[2] Dr. S. Kannan, Vairaprakash Gurusamy, "Preprocessing Procedures for Content Mining", 05 Walk 2015.
[3] Shalinda Adikari and Kaushik Dutta, Distinguishing Fake Profiles in LinkedIn, PACIS 2014 Procedures, AISeL
[4] Z. Halim, M. Gul, N. ul Hassan, R. Baig, S. Rehman, and F. Naz,"Malicious users' circle discovery in social organize based on spatiotemporal co-occurrence," in Computer Systems and Data Innovation (ICCNIT),2011 Universal Conference on, July, pp. 35–390.
[5] Mahmood S, Desmedt Y," Blurb: preparatory investigation of google?'s security. In: Procedures of the 18th ACM conference on computer and communications security", ACM 2011, pp.809–812.
[6] Stein T, Chen E, Mangla K," Facebook resistant framework. In: Procedures of the 4th workshop on social arrange systems", ACM 2011, pp
[7] J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, B. Zhao, Understanding idle intuitive in online social systems, in: Procedures of the 10th ACM SIGCOMM Conference on Web Estimation, ACM, 2010, pp. 369– 382
[8] Kazienko, P. and K. Musiał (2006). Social capital in online social environment.Wisdom-Based Cleverly Data and Building Frameworks, Springer.
[9] Saeed Abu Nimeh,T.M.Chen,and O.Alzubi,"Malicious and spam post in online social network,"computer, vol44, no.9, IEEE2011,pp.23-28
[10] Determining Degree of Visual Center of Human Consideration Utilizing Machine Learning Methods by P. Chakraborty, M. A. Yousuf, and S. Rahman. In: Procedures of the Worldwide Conference on Patterns in Computational and Cognitive Designing, Springer, Singapore, 683-694. Shamim Kaiser, Bandyopadhyay, Mahmud, and Raym, editors. https://doi.org/10.1007/978-981-33-4673-4 56
[11] Zero-Shot Learning to Recognize Thing Occasions from Obscure Picture Sources. Muzammel, C.S., Chakraborty, P., Akram, M.N., Ahammad, K., and Mohibullah, M. (2020).IJITEE, 9, 988–991. Universal Diary of Inventive Innovation and Investigating Designing. https://doi.org/10.35940/ijitee.C8893.029420
[12] Utilizing Format and Hoard Include Coordinating, Sultana, T. Ahmed, P. Chakraborty, M. Khatun, M. Hasan, and M. S. Uddin distributed Protest Location in 2020. IJACSA, 11, 233-238. Universal Diary of Progressed Computer Science https://doi.org/10.14569/IJACSA.2020.0110730
[13] Utilizing machine learning procedures, Faruque, M.A., Rahman, S., Chakraborty, P., Choudhury, T., Uh, J.S., and Singh, T.P. (2021) find out the extremity of the public's suppositions on cricket https://doi.org/10.1007/s41324-021-00403-8
[14] Utilizing a machine learning approach based on Twitter information, Sarker, Chakraborty, Sha, Khatun, Hasan, M.R., and Banerjee (2020) created an extemporized method for information examination and fear based oppressor assault detection.8, 50–62, Diary of Computing and Communications.
[15] Distinguishing Fake Accounts on Social Media, S. Khaled, N. El-Tazi, and H.M. Mokhtar, 2018. Huge Information 2018 IEEE Universal Conference, Seattle, 10–13 December 2018. https://doi.org/10.1109/BigData.2018.8621913
[16] Social Systems Fake Profiles Location Utilizing Machine Learning Calculations, Y. and Z. Elyusufi, 2019. In: Advancements in Keen Cities Applications



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY