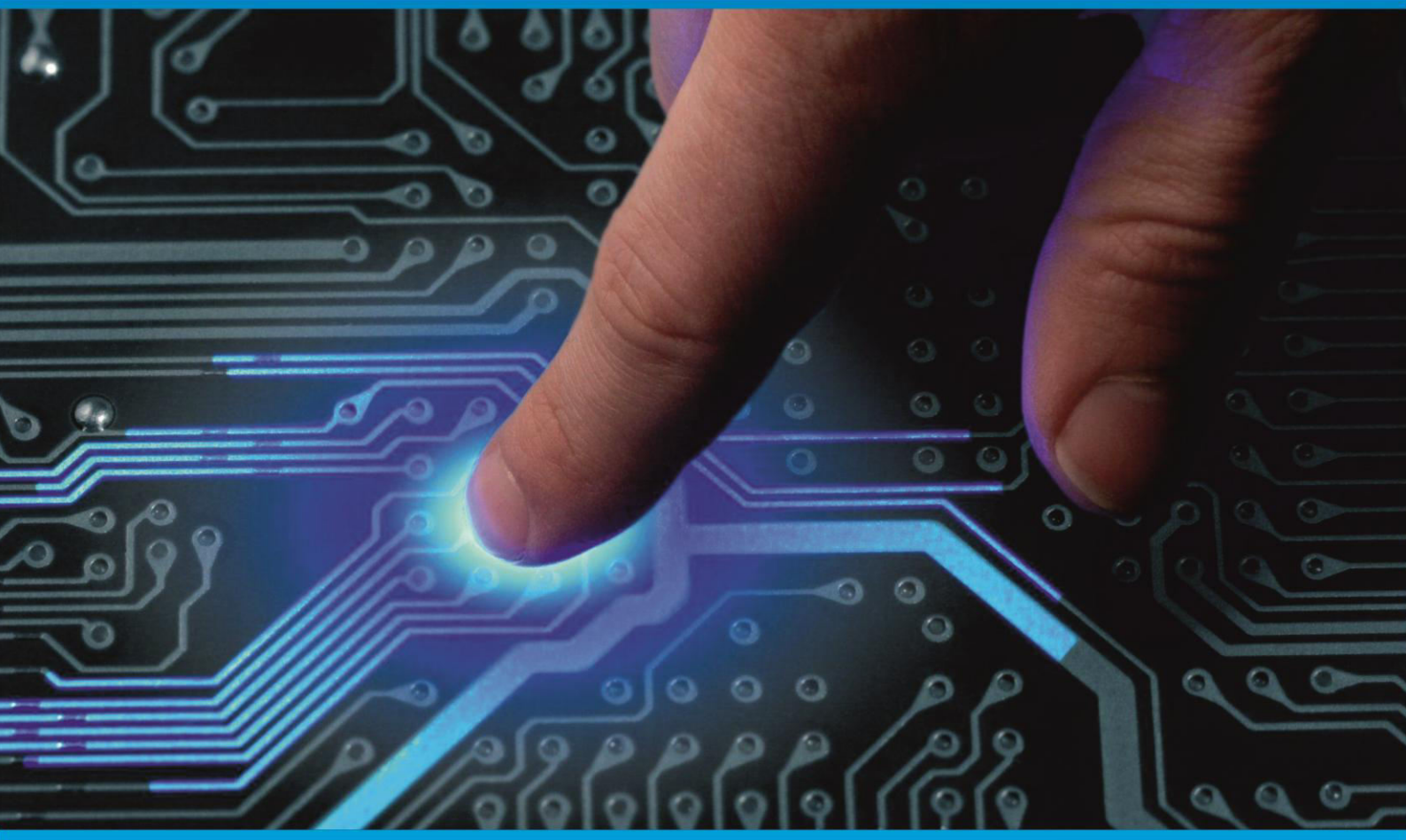
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

Detection of Clone and Fake Accounts in Social Media: A Survey

Prof. Jyothi Neeli, Akash R, Chaitra A, Swaroop Raj, Yashas Gowda

Dept. of Information Science and Engineering, Global Academy of Technology, Visvesvaraya Technological University, Bengaluru, Karnataka, India

ABSTRACT: Online social network (OSN) is a network hub where people with similar interests or real-world relations interact. With the increase in popularity of OSN's, security and privacy issues related to it are also increasing. It has fostered the emergence of a new spam market. The significant increase in illegal activities on these social-platform have induced threat to personal information about the users. There are various illegal activities, active on online social networks every day. Illegal activities include cloning of profiles which is then misused to damage the identity of the victim user, phishing, stalking, spamming through fake accounts etc. Clone profile attack is where identity theft of a profile is done to create a copy of the profile. Fake profile is the creation of profile in the name of a person or company who/which do not exist. It is done to carry out malicious activities. The detection of such profiles without affecting genuine user profiles is a challenge.

KEYWORDS: online social media, similarity measures, Levenshtein distance, classification algorithm, threshold

I. INTRODUCTION

Online social network like Facebook, Twitter, Instagram is used all over the world by billions of people. Users share a lot of personal information on their social media accounts. The enormous amount of information available on these platforms are not all secured and taken care of. An entire industry of black-market services has come to existence which offers fake account-based services for sale. Intruders and harm seekers are always finding ways to invade the privacy of victims to damage their identity and cause distress to them and their loved ones. Most of the online social network users are unaware of the threats that are existing. Profile cloning is one of the types of attack. There are two types of cloning, same site and cross site profile cloning. If user credentials are taken from one Network to create a clone profile in same Network then it is called Same Site profile cloning. In Cross Site profile cloning, attacker takes the user information from one Network to create a duplicate profile in other Network in which the user is not having any account. Fake account means that the accounts that do not belong to real humans, the one which can present fake news, wrong web ratings, aggressive following behaviours. These accounts are the ones that violate the twitter rules and act in a prohibited manner.

II. LITERATURE SURVEY

Social network sites such as Twitter and Facebook have millions of users across the world, which has led to the interrelation of their social and personal life. Social sites have led to various problems such as fake pots and accounts that impact on real life events. The detection of fake account on twitter, using classification algorithms, twitter account analysis, similarity measures and decision tree-based algorithms is proposed using a minimized dataset [1]. Dataset are used to compare methods and their changes to the similarity-based learning. This study can be applied on different social network sites with minor changes with accordance to the nature of network [2].

Machine learning is a domain where in the computers are provided with the ability to learn without being explicitly programmed. A similarity measure is a method of finding similar contents between two or more objects [2]. Cosine similarity, Jaro ratio, Jaccard ratio, Levenshtein distance and hamming distance are used for the calculations of similarity measures. Levenshtein distance between two words is the minimum number of single-character updates required to change one word into the other. All the above-mentioned algorithms cannot give more weightage to the matching, different algorithms are used for different attributes such as name, age, email, etc.

A pre-processed dataset using a supervised discretization technique known as entropy minimization discretization (EMD) on the numerical features is put to action which further analyses the results of the Naïve Bayes algorithm [3]. A

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

manually collected dataset is used and investigated by a group of people. description attributes, protected attributes, verified attributes, followers and following count and various other factors taken into picture is used for finding the fake account on social media. Description attribute is the length of the user defined string describing the account [3]. Protected attributes are the ones that the users decide that no other user other than the selected followers can see. Verified attributes are the ones that are stated true after the user is verified by the respective site.

As a result of a few projects, the proposed architecture for detection of fake and clone profile is similar to that of the below mentioned diagram [4]. This architecture has four phases.

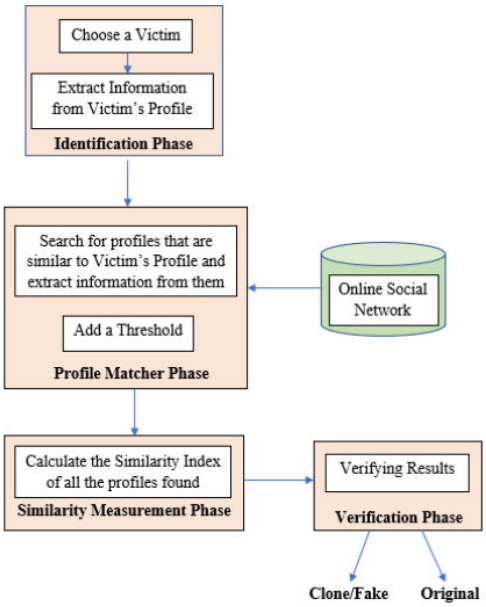


Fig.1 Architecture design for fake and clone account detection

- Identification phase – the victim profile is chosen and the user information such as name, location etc are extracted, termed as user identifying information and passed on to the next phase.
- Profile matcher phase – online search engines are used to search the profiles with the same name as the victim profile. Name being taken as the primary attribute. If results after such a search is more in number, more attributes are added and the clone profile is detected, if any exists.
- Similarity measurement phase – similarity index is calculated between the found and victim profiles, which is then compared with the threshold value. If similarity index is found to be greater than the threshold value, it is passed on to the verification phase else its discarded.

Two types if similarities are calculated: attribute similarity and network similarity.

- Verification phase – in this last step the user verifies the results manually, and declare it fake or original. The most important parameter to be set is the threshold, because with too many alarms it will be difficult to verify all profiles manually [4].
- Sowmya P and MadhumithaChatterjeein their work [5], state a different approach in detection of clone profiles, using C4.5 algorithm along with similarity index is calculated to detect clone accounts, and a comparision is made to check how well these two methods help detecting clone accounts. C4.5 is a classification based decision tree algorithm. A decision tree is built based on the given data and at each node the attribute that effectively splits the sample sets to subsets is chosen. Information gain and entropy are the splitting factors used. C4.5 algorithm find the similarity between the attributes by building a tree like structure [5]. The profile is compared with the profiles in the database, and if it matches it is declared as clone, else not clone. Four evaluation metrices are used to evaluate the performance of the system. True positive, true negative, false positive, false negative are the four standard indicators [5]. True positives are records that are correctly detected with expected errors. True negative are records correctly detected expected as neutral. False positives are records detected by the system as expected but are actually listed in the other vectors and false negatives are records not detected by the system.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

In a machine learning approach [6], characteristics are used as attributes to machine learning algorithms as to classify fake and genuine users. A variety of prohibited behaviours that violate the twitter rules is a twitter spam [6]. Social spammers use one to many communication methods to spread spam quickly. In order to use machine learning approaches, we need a pre-classified labelled collection of users as fake and genuine. Fake users are said to exhibit a unique behaviour pattern on OSN. Cumulative distribution function (CDF) is used on a bunch of attributes to classify as fake or genuine.

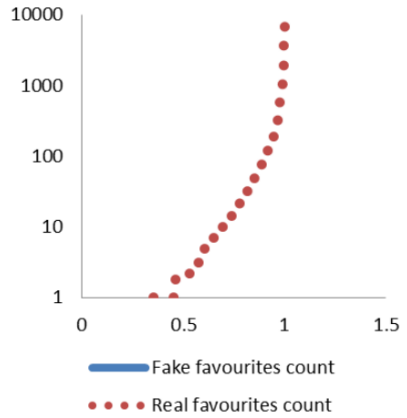


Fig.2 CDF for the number of tweets fake and real accounts favoured

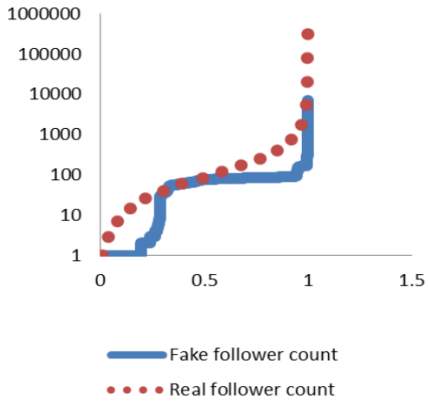


Fig.3 CDF for the number of tweets fake and real accounts have posted

The above graphs serve as examples for the CDF used, where the x-axis represents the CDF and y-axis represents the attributes for both the fake and real followers and is represented in a logarithmic scale. Fig.2 shows that the real users have more number of followers than fake accounts. From Fig.1 it is clear that number of tweets the fake followers favoured is zero. Attributes as such are considered and CDF graph is drawn to distinguish fake and real followers. Machine learning algorithms are required for the detection of fake accounts on social media [6].

With strict privacy settings and evolving of API it is hard to extract data from online social media accounts. [7] has contributed to face such difficulties by extracting user information form such a platform-Facebook. It has made use of 17 such features for the detection of fake users from real ones, and is able to identify the type of activities that contribute the most in fake user detection. 17 features are then fed into learning algorithms such as k-nearest neighbour, naïve bayes, random forest etc. All the activities on feeds are captured as JSON objects [7]. Performance evaluation of the 12 learning algorithms were made to learn which among them is the best and is concluded from the following figure that the classifier accuracy of close to 80% is achievable by making use of conventional learning classifiers. The classifiers with detection rate over 75% are shown.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

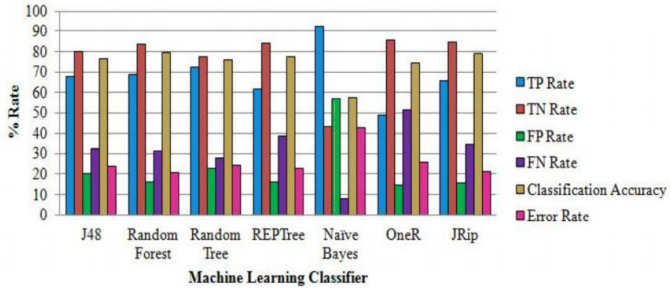


Fig.4 Detection rate of various classifiers

S.P.Maniraj in his journal[8] has used stable factors such as spam commenting, artificial activity and engagement rate is considered to detect if a account is fake or genuine. A recent survey suggested that the number of accounts present in the social media is much greater than the users using it [8]. This research has made use of gradient boosting algorithm with decision tree considering the three above algorithms. The new techniques used for creating the fake accounts may not match with the application or software used for detecting the same. The exceptional improvement in creating of fake accounts requires different approaches to find them as well. Gradient Boosting Algorithm is used, which works similar to that of Random Forest Algorithm. This algorithm is used because of its improved capability of giving the output even if some inputs are missing.

Web scrapping is used to extract data from online social sites. Information such as login activity, total likes, total comments, number of posts, number of followers, number of following is extracted and the calculation of engagement rate is done. An engagement rate is a metric that measures the level of engagement of a post or story received on social media. Engagement rate percentage is calculated by the following formula.

$$\text{Engagement rate percentage} = \left(\frac{\text{Total number of interactions}}{\text{Total number of followers}} \right) \times 100$$

Regular social media activities such as commenting, liking is called an artificial activity when the frequency of the engagement rate is very high. Gradient boosting algorithm is fed with the necessary data and with a lot of training data this algorithm gives accurate output. The best feature of the algorithm is that it gives perfectly predicted output even in the absence of few inputs [8].

The summary of the literature survey along with the used methodologies is discussed in the following table:

Sl.no	Authors	Techniques	Contributions	Limitations
1	Ahmed El Amira [1]	The proposed method consists of two ain steps. First is to determine the main factors that influence correct detection and second step is to apply a classification algorithm to determine the fake account.	The proposed approach has reached seven effective attributes for fake account detection with high accuracy.	According to unique nature of each social network, the system claims fake accounts can be detected making minor changes, but a dataset needs to be prepared to prove this claim.
2	Arpitha D [2]	The proposed method includes applying similarity measure algorithms between two datasets and construction of decision tree	Similarity measures is alone used to detect the clone accounts.	All algorithms inclusive cannot give more weightage to the matching

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

3	BuketErsahin [3]	The proposed methodology includes preparing a own dataset created manually and examined and the common decisions are put in the dataset. Decision attributes, protected attributes, friends count, status count etc. are all considered and the decision of a fake account is made.	The EMD is used to discretize the data with minimal description length as the stopping criteria. There is increased accuracy with naïve bayes by pre-processing the dataset by using discretization technique on selected features.	The study can be enhanced by applying our fake account detection methodology in other social media platforms by trying similarity algorithms and feature selection which can improvise on the search results.
4	Sowmya P [4]	The entire methodology is divided into four phases namely, identification phase, profile matcher phase, similarity measurement phase and verification phase	n-gram similarity is used to which enables us to compare attributes in which order of words is taken into consideration. Extraction of data from Facebook and Twitter API's is done	To set the threshold is very important or with too many alarms it will be difficult to check all profiles manually for clone or fake
5	Sowmya P [5]	C4.5 decision tree algorithm is used for classification. Cosine similarity as well as levenshtein distance are the techniques used to detect clone accounts	Datasets are collected from MIB projects and are used for the experiments. Evaluation metrics are done based on true positive, true negative, false positive and false negative	NLP can be used taking the tweets into consideration to increase the precision to which such accounts can be detected
6	Ashraf Khalil [6]	A labelled dataset with pre classified fake or genuine accounts is created. The fake followers exhibit a unique behaviour pattern in twitter. The CDF is then applied to the attributes. The attribute selection is done as to classify the dataset as fake and genuine followers.	The number of characteristics that distinguish fake and genuine is identified, and so are used as attributes to have gained the highest detection accuracy using machine learning algorithms.	This machine learning approach cannot be used in other social networks by making minor changes. The detection of fake accounts highly depend on the content and user-behaviour attributes.
7	Aditi Gupta [7]	The proposed methodology includes data collection, feature identification and learner classifiers.	User actions such as likes, comments and shares has been taken as the maximum contribution to detect fake accounts.	More number of classification algorithms to be applied on larger number of datasets to improve detection accuracy is to be done.
8	S.P.Maniraj[8]	Web scraping is done to extract information such as login activity, number of followers and followings etc. and calculation of engagement rate is done. Artificial activity and spam comments are now considered and fed to the classification algorithm	Spam commenting, engagement rate and artificial activity are the base attributes considered for the classification algorithm Gradient Boosting algorithm	Due to the consideration of stable factors, basic user details are not taken into account which may cause a slight disturbance in the decisions taken for such accounts

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905069 |

III. CONCLUSION

There is a proportional increase of social media users and the threats and security issues caused on social media platforms with the creation of fake, clone, user-misclassified accounts. It is important to develop techniques for the detection of such accounts. Various similarity measures such as network similarity and attribute similarity are measured to distinguish between the real and fake accounts.

Machine learning algorithms are deployed by various systems. In this paper we have done a literature survey of various such models and methodologies adapted to conclude which is the best suited version of them all for the best results in detecting fake and clone accounts. The best algorithm to do so will be the one which considers minimum features, is less time consuming when it comes to large amount of data and is more accurate in its results.
In future work, NLP can be used to scan through the comments posted and/or through the messages exchanged for early detection of such accounts.

REFERENCES

1. Ahmed El Azab, Amira M. Idress, Mahmoud A, Hesham Hefny, “Fake Account Detection in twitter based on Minimum Weighted set”, 2016 International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:1
2. Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A.S, “Python based Machine Learning for Profile Matching”, International Research *Journal* of Engineering and Technology (IRJET), 2018
3. BuketErşahin, OzlemAktaş, Deniz Kilinç, Ceyhun Akyol, “Twitter fake account detection”, 2017 International *Conference* on Computer Science and Engineering (UBMK)
4. Sowmya P and MadhumitaChatterjee ,” Detection of Fake and Cloned Profiles in Online Social Networks”, Proceedings 2019: *Conference* on Technologies for Future Cities (CTFC)
5. Sowmya P and Madhumita Chatterjee, “Detection of fake and clone accounts in twitter using classification and distance measure algorithms”, International *Conference* on Communication and Signal Processing, July 28 - 30, 2020
6. Ashraf Khalil, Hassan Hajjdiab and Nabeel Al-Qirim, “Detecting Fake Followers in Twitter: A Machine Learning Approach” 2017 International *Journal* of Machine Learning and Computing
7. Aditi Gupta and Rishabh Kaushal, “Towards Detecting Fake User Accounts in Facebook”, 2017 ISEA Asia Security and Privacy (ISEASP)
8. S.P.maniraj, Harie Krishnan G, Surya T, Pranav R,”Fake account detection using machine learning and datascience”, International *Journal* of innovative technology and exploring engineering (IJITEE), Nov-2019
9. Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and JariVeijalainen, “Detection of fake profiles in social media”, In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017), pages 363-369, 2017
10. Mauro Conti, Radha Poovendran and Marco Secchiero, “FakeBook: Detecting Fake Profiles in On-line Social Networks”, 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining
11. Aditi Gupta and Rishabh Kaushal, “Towards Detecting Fake User Accounts in Facebook”, 2017 ISEA Asia Security and Privacy (ISEASP)
12. Stefano Cresci, Roberto Di Pietro, MarinellaPetrocchi, AngelloSpognardi, Maurizio Tesconi, “Fame for sale: Efficient detection of fake Twitter followers”, 2015 Elsevier’s journal Decision Support Systems, Volume 80
13. OanaGoga, Patrick Loiseau, Robin Sommer, “On the Reliability of Profile Matching Across Large Online Social Networks” In the Proceedings of International Conference.
14. SuprajaGurajala, Joshua S. White, Brian Hudson, and Jeanna N. Matthews, "Fake Twitter accounts: Profile characteristics obtained using an activity-based pattern detection approach," in SMSociety '15, July 27 - 29, Toronto, ON, Canada, 2015
15. The Fake project. (Online). http://wafi.iit.cnr.it/theFakeProject/ (last retrieved on 30-10-2015).
16. Qiang Cao, Michael Sirivianos, Xiaowei Yang, and Tiago 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, 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details