iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** XII **Month of publication:** December 2020

DOI: https://doi.org/10.22214/ijraset.2020.32627

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: 7.429
Volume 8 Issue XII Dec 2020- Available at www.ijraset.com

A Review on Fake Account Detection in Social Media

Khushboo Saraswat[1], Dr. Nirupma Tiwari[2]
[1]*Department of CSE, SRCEM, RGPV University Bhopal India*
[2]*Department of CSE, SRCEM, RGPV University Bhopal India*
khushboosaraswatsrcem96@gmail.com[1]
girishniru@gmail.com[2]

Abstract: ***Social media sites are used on a regular basis in today's world, and have become an integral part of our lives. It is one of the main means of communication, and has become a tool for both spammers and scammers. Such social media platforms have changed drastically how we live our social life. It has become easier to make new friends, keep in touch with them, and know their updates. But many problems, such as fake profiles and online impersonation, have also grown with the rapid growth of social media. This paper presents a review of various existing methods for detecting fake accounts in social media. In this paper a study is carried out of different research papers and provides a comparative study of existing work done. Fake accounts are mostly used by intruders to perform malicious activities such as personal identity harm, theft and privacy intrusion on social media platforms. Hence identifying an account is either real or fake is one of the key issues.***
Keywords: Social Media, Fake accounts, Machine learning algorithms, Comprehensive Review.

I. INTRODUCTION

These days, social media is rising extremely fast. It is very important for marketing companies who aim to promote themselves by creating a base of followers and fans. Social Media [2] such as Facebook and Instagram have become increasingly popular and vital part of today's era. In addition the use of social media as a means of communication, it is often used to boost popularity and support businesses. At first glimpse, the popularity of an account is measured by some metrics such as follower count or shared contents such as the number of likes, comments or views. Social media [4] are great platforms for our lives, but there are a number of issues which need to be addressed. Issues related to social media, such as confidentiality, online abuse, misuse and bullying, etc. are most commonly used by fake accounts that appear to have been generated on behalf of organizations or individuals , which can damage reputation and reduce the number of likes and followers of individuals. On the other hand fake account creation is expected to cause more damage than any other form of cyber crime.

There are several reasons for making fake accounts on social media [12] introduces some reasons.
Some reasons why people make fake accounts are:

A. Social Engineering
B. Online impersonation
C. Advertising and Campaigning
D. Privacy Intrusion etc.

Generally, all social media spammers are legal users. It is therefore a challenge to recognize them, in addition to recognizing them from legal users. Moreover, fraudsters can still use cheap automated approaches. Acquiring credibility in addition to trust and making it hard for the vast population of social media users to perceive. Social media fake account identification is a classification problem in which legal users are well recognized from fake user on the basis of their corresponding features. Identity is an attribute that is connected to a human being, apart from him or her.

A common example is a person's name. Another example is a passport. Contains the name, date of birth and place of the person, citizenship, digitally captured fingerprints and a digitally captured photograph of the person. In general, [7] identity should be unique in the sense that each object of identification must refer only to a maximum of one person. The same person may still have several identities, such as a passport or a social security number. True identification is checked by the authorities of a nation state. A modern passport is a typical example of that. Authorities guarantee that the image, fingerprints, name, date of birth etc. belong to the same person , i.e. confirm the attachment of the item. A person is typically identified by a profile on a social media platform. This normally includes an image and a name, probably an address and a date of birth. The platforms are not, However, make sure that the

identity person referred to in the profile is actually generated and regulates the profile. If that's not the case, somebody using the name of someone else. It's considered a false identity.

Several detection approaches have been proposed, [18] which can fall into three categories:

1) features learning process,
2) social network-based process and
3) optimization process

The first two kinds of methods just consider features learning or social network knowledge, yet the performance of fake profile detection is not optimal. The third method uses both features as well as social network knowledge to learn an optimized model.

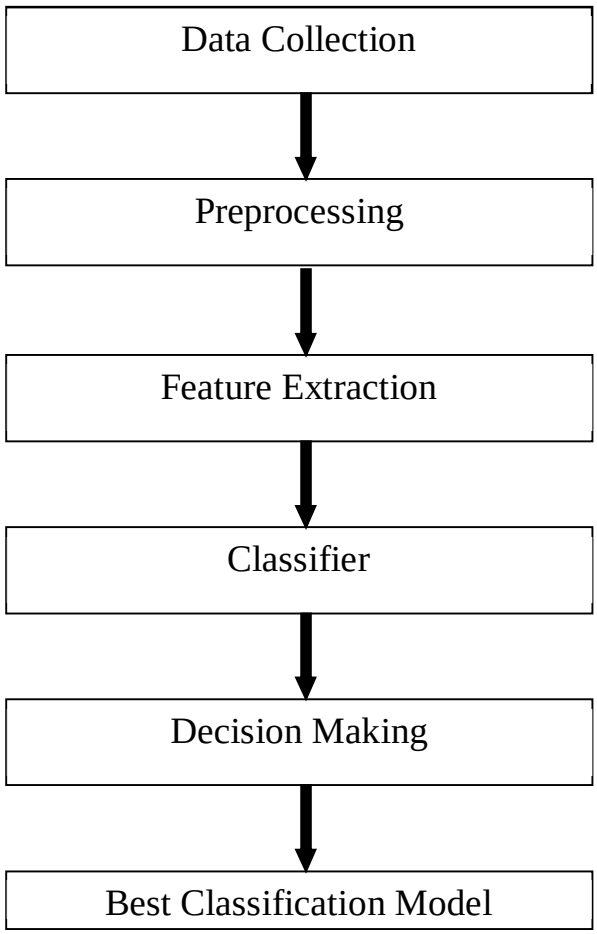


Figure 1.Research Steps involved in Fake Account Detection in social media.

False identities play a significant role [7] in Advanced Persistent Threats (APTs), i.e. organized, persistent and nuanced attempts to compromise targets in Governmental organizations, non-governmental organizations, and business organizations. False identities are most often used in other harmful practices, such as spamming, deliberately inflating the number of users in a promotional application, etc.

One of the biggest problems with social media [9] is that spammers can use their identities for different purposes. One of these aims is to spread rumors that may influence a particular organization or even a large scale community.

Fake accounts have some characteristics through which they are identified. [2] mention some common characteristics of fake account which are listed below :

a) Have a high following and low follower count

b) Absence of profile picture
c) The odd names of users
d) Liking behavior

II. LITERATURE REVIEW

Recent studies have focused on related research issues and have contributed a significant amount of work to the study of a different aspect of social media.

Yasyn Elyusufi et al.[2020] This paper proposed an approach to the detection of a false profile on the social media site using minimal profile data. The proposed model was trained independently using the supervised learning algorithm for datasets, including fake and legitimate users.

The ensemble classifier was used to make predictions more accurate. Three supervised machine learning algorithms are used in this research work. Random Forest, Decision Tree and Naive Bayes are used to identify false and genuine profiles. The result shows that the Random forest algorithm is better than the other Algorithm with a precision score of 99.64 %. [4]

Farhan Nurdiatama Pakaya et al. [2019] Throughout this work, a classification model has been developed using only account tweets that differentiate legitimate accounts from fake accounts. Four different algorithms are used in this paper such as Logistic Regression, ADA Boost, XG Boost, Random Forest.

Model evaluation of this research reveals that XG Boost with tf- idf features is the best layout for the binary classification scheme and the best model for multiclass classification is world2vec features. This work has managed to achieve a maximum accuracy of 95.5 %. [1]

Fatih Cagatay Akyon , M. Esat Kalfaoglu [2019] This paper analyzes the identification of false and robotic accounts that lead to a fake Instagram collaboration as a binary classification issue. This paper proposed a derived function for fake and automated account recognition and a cost sensitive feature extraction technique based on a genetic algorithm for choosing the best features for the classification of automated accounts.

To detect fake and automated accounts several machine Learning algorithms such as Naive Bayes, logistic regression, support Vector machines and neural networks are used. The SVM and neural networks obtained the most successful F1 score.SVM obtained 86 % and the neural network obtained the highest F1 score with 95 %. [2]

Mohammed Basil Albayati, Ahmad Altamimi [2019] Proposed a model that uses a range of data mining techniques to detect false profiles. A set of supervised (ID3 decision tree, K-NN and SVM) and unsupervised (K-Means, K-Medoids) machine learning algorithms has been applied to 12 behavioral and non-behavioral discriminatory profile attributes. The results showed that ID3 had an accuracy rate of 97.76 % in the detection process. [5]

S.P. Maniraj et al.[2019] proposed a new method to identify fake accounts on online social media. A decision tree containing three attributes is used in this gradient boosting algorithm.

These attributes are spam commenting, artificial activity and engagement rate. In this paper the process of identifying a fake account mainly depends on factors such as engagement rate and artificial activity. [11]

Zulfikar Alom et al.[2018] Proposed a new and more powerful collection of features to identify twitter spammers. It demonstrated both graph-based and tweet-based characteristics and applied them to seven different machine learning algorithms, such as K-NN, Decision Tree, Naive Bayes, Random Forest, Logistic Regression, Support Vector and Extreme Gradient Boosting (XG-Boost). The study reveals that the Random Forest algorithm achieves a better performance compared to other algorithms with an accuracy of 91%. [6]

Mohd Fazil , Muhammad Abulaish [2018] Integrated methodology with added categories of features such as metadata, content-based interaction and content-based attributes to previously defined community-based features for the recognition of auto spammers was discussed in this paper.

The uniqueness of this strategy is that users have been classified on the basis of their exchanges with their followers as ignoring the contents of the followers and the characteristics of metadata were practically difficult. The experiment consisted of a real-world dataset containing legitimate users as well as spammers whose profiles were distinguished by 19 predefined attributes along with 6 newly specified and 2 redefined features.

The results showed that both interaction-based and community-based classifications proved to be effective whereas metadata classification was the least efficient. [3]

Ahmed El Azab et al.[2016] A classification method for identifying fake accounts on twitter is present in this paper. The study identifies a minimised set of key factors that influence the identification of a fake account on twitter and then decides which are

applied using different classification techniques. In this paper, the classification method used are Random Forest, Decision Tree, Naive Bayes, neural network, Support vector Machine. [10]

III. COMPARATIVE STUDY

In this study, comparison of different existing techniques and accuracy score is shown below :

Table 1.Comparison table of existing techniques and accuracy

Ref.	Year	Author	Technique	Accuracy
[19]	2015	Cao Xiao et al	Random forest, Support Vector Machine, and Logistic regression	95%
[8]	2017	Ashraf Khalil et al	Support Vector Machine, Simple Logistic , Instance-Based classifier using 1 nearest neighbor	98.74 %
[9]	2017	Buket Erşahin et al	Naïve Bayes	90.41 %
[6]	2018	Zulfikar Alom et al	Decision Tree, Naive Bayes , Random Forest, Logistic Regression,K-NN, Support Vector Machine and Extreme Gradient Boosting (XG-Boost).	91%
[21]	2018	Sarah Khaled et al	Support Vector Machine, Neural Network, SVM-NN	98%
[1]	2019	Farhan Nurdiatama Pakaya et al	Logistic Regression, ADA Boost, XG Boost, Random Forest	95.5%
[16]	2019	Hakimi A.N. et al	K-NN, SVM, NN	82%
[4]	2020	Yasyn Elyusufi et al	Random Forest, Decision Tree and Naive Bayes	99.64%

IV. DATASET DESCRIPTION

In the dataset that we want to use in our research have the selected base features which are listed below:

A. Existence of profile photo
B. Username of the profile
C. Whether the account is private or not
D. The number of followers of the account
E. Following Count of the account
F. Whether or not the account has an external URL .
G. Media posting

V. PROPOSED PLAN

Our objective is to effectively identify the fake account on social media with the possible minimum set of attributes and with highest accuracy. In our study the first step is to identify the key factors that influence the correct identification of fake account and second step is to apply a combination of classification algorithm. The main objective of this research is to design an algorithm that performs higher and will improve the efficiency of prevailing system.

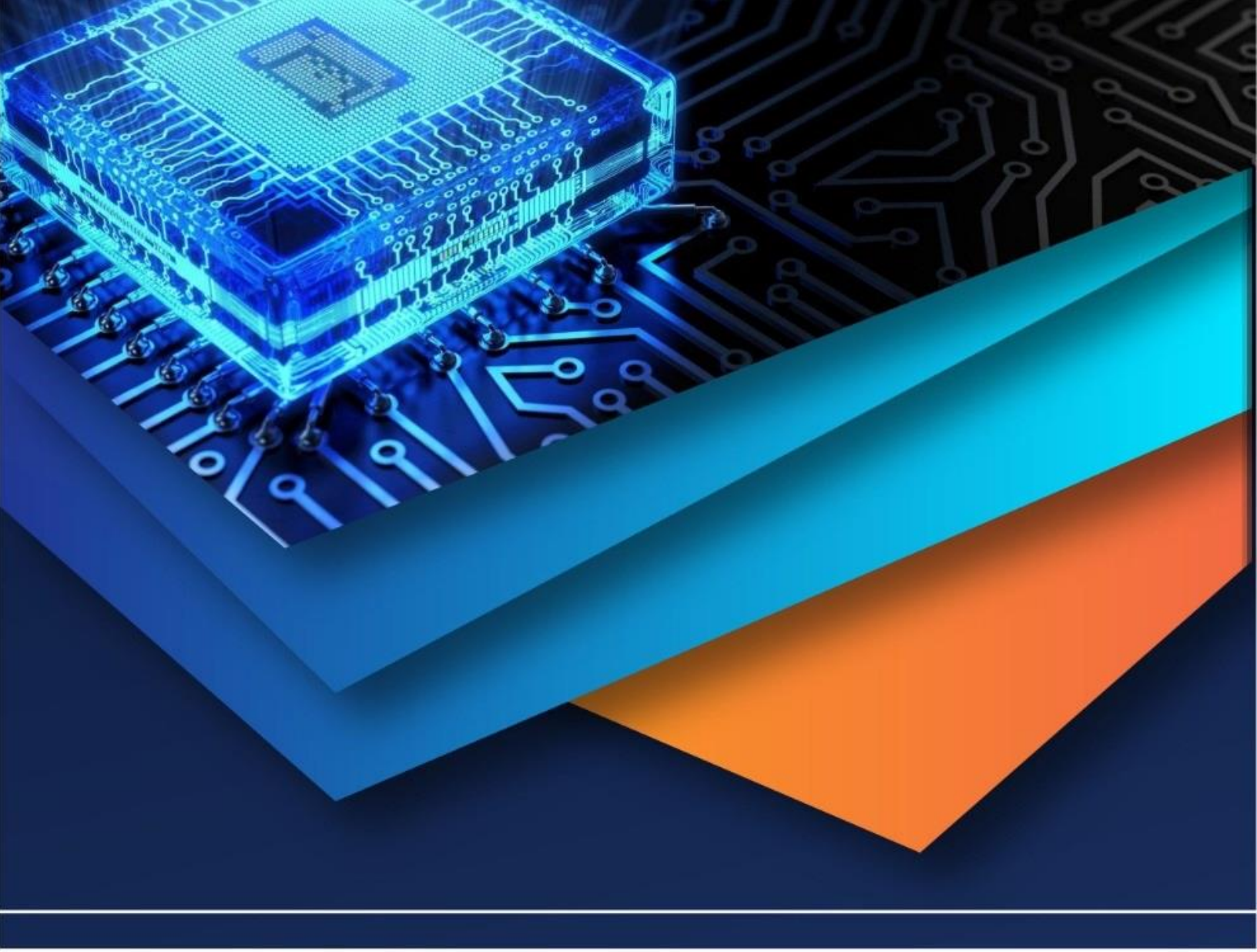
VI. CONCLUSION

This paper presents a review of different research papers in which classification techniques are used for performing the detection of fake account in social media. There are different classification algorithms used in different research like Support Vector Machine,

Random Forest, Logistic Regression, Decision Tree, Naïve Bayes, Neural Network, XG-Boost, ADA Boost and K-NN. Best performance according to our study is achieved by Random Forest with an accuracy score of 99.64 % and Random Forest is one of the most commonly used machine learning algorithms, due to its simplicity and the fact that it can be used for both regression and classification problems.

REFRENCES

[1] F. N. Pakaya, M. O. Ibrohim and I. Budi, "Malicious Account Detection on Twitter Based on Tweet Account Features using Machine Learning," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 2019, pp. 1-5, doi: 10.1109/ICIC47613.2019.8985840.
[2] F. C. Akyon and M. Esat Kalfaoglu, "Instagram Fake and Automated Account Detection," 2019 Innovations in Intelligent Systems and Applications Conference (ASYU), Izmir, Turkey, 2019, pp. 1-7, doi: 10.1109/ASYU48272.2019.8946437.
[3] M. Fazil and M. Abulaish, "A Hybrid Approach for Detecting Automated Spammers in Twitter," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2707-2719, Nov. 2018, doi: 10.1109/TIFS.2018.2825958.
[4] Elyusufi, Yasyn & Elyusufi, Zakaria & M'hamed, Aït Kbir. (2020). Social Networks Fake Profiles Detection Using Machine Learning Algorithms. 10.1007/978-3-030-37629-1_3.
[5] Albayati, Mohammed & Altamimi, Ahmad. (2019). Identifying Fake Facebook Profiles Using Data Mining Techniques. Journal of ICT Research and Applications. 13. 107-117. 10.5614/itbj.ict.res.appl.2019.13.2.2.
[6] Z. Alom, B. Carminati and E. Ferrari, "Detecting Spam Accounts on Twitter," 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Barcelona, 2018, pp. 1191-1198, doi: 10.1109/ASONAM.2018.8508495.
[7] Romanov, Aleksei & Semenov, Alexander & Mazhelis, Oleksiy & Veijalainen, Jari. (2017). Detection of Fake Profiles in Social Media - Literature Review. 363-369. 10.5220/0006362103630369.
[8] Ashraf Khalil, Hassan Hajjdiab, and Nabeel Al-Qirim, "Detecting Fake Followers in Twitter: A Machine Learning Approach," International Journal of Machine Learning and Computing vol. 7, no. 6, pp. 198-202, 2017.
[9] B. Erşahin, Ö. Aktaş, D. Kılınç and C. Akyol, "Twitter fake account detection," 2017 International Conference on Computer Science and Engineering (UBMK), Antalya, 2017, pp. 388-392, doi: 10.1109/UBMK.2017.8093420.
[10] Elazab, Ahmed & Mahmood, Mahmood & Hefny, Hesham. (2016). Fake Account Detection in Twitter Based on Minimum Weighted Feature set. International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:1, 2016.
[11] S. P. Maniraj, Harie Krishnan G, Surya T, Pranav R (2019). Fake Account Detection using Machine Learning and Data Science. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November, 2019.
[12] Bharat Sampatrao Borkar, Dr. Rajesh Purohit (2019).Recognisation of fake profiles in social media. Department of Computer Science & Engineering School of Engineering & Technology, Suresh Gyan Vihar University, Jagatpura, Volume-9 Issue-2,2019.
[13] Adikari, S. and K. Dutta. "Identifying Fake Profiles in LinkedIn." ArXiv abs/2006.01381 (2014).
[14] Devakunchari Ramalingam, Valliyammai Chinnaiah,"Fake profile detection techniques in large-scale online social networks: A comprehensive review" ,Computers & Electrical Engineering, Volume 65,2018.
[15] K. Zarei, R. Farahbakhsh and N. Crespi, "Typification of Impersonated Accounts on Instagram," 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), London, United Kingdom, 2019, pp. 1-6, doi: 10.1109/IPCCC47392.2019.8958763.
[16] Hakimi, A.N., Ramli, S., Wook, M., Zainudin, N.M., Hasbullah, N.A., Wahab, N., & Afiza, M.R. (2019). Identifying Fake Account in Facebook Using Machine Learning. IVIC.
[17] F. Masood et al., "Spammer Detection and Fake User Identification on Social Networks," in IEEE Access, vol. 7, pp. 68140-68152, 2019, doi: 10.1109/ACCESS.2019.2918196.
[18] H. Shen and X. Liu, "Detecting Spammers on Twitter Based on Content and Social Interaction," 2015 International Conference on Network and Information Systems for Computers, Wuhan, 2015, pp. 413-417, doi: 10.1109/ICNISC.2015.82.
[19] Xiao, Cao et al. "Detecting Clusters of Fake Accounts in Online Social Networks." AISec '15 (2015).
[20] N. Singh, T. Sharma, A. Thakral and T. Choudhury, "Detection of Fake Profile in Online Social Networks Using Machine Learning," 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE), Paris, 2018, pp. 231-234, doi: 10.1109/ICACCE.2018.8441713.
[21] S. Khaled, N. El-Tazi and H. M. O. Mokhtar, "Detecting Fake Accounts on Social Media," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 3672-3681, doi: 10.1109/BigData.2018.8621913.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY