Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 4; 2025; Page No. 149-152

Received: 01-04-2025
Accepted: 09-06-2025

The Study Analyzes the Evolution of Social Networking Globally and Nationally, Employing the Kolmogorov-Smirnov Test and Chi-Square Test to Assess Various Online Platforms

[1]Harpreet Singh and [2]Krishan Kumar

[1]Research Scholar, Shri Krishna University, Chhatarpur, Madhya Pradesh, India
[2]Professor, Department of Computer Science, Shri Krishna University, Chhatarpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.18440634

Corresponding Author: Harpreet Singh

Abstract

The Internet has grown in importance and impact over the years, causing people to become more reliant on it. As its user base continues to grow, the Internet poses more and more risks to computer systems' security. Over the last decade, the number of these computing systems including desktops, laptops, smartphones, and the Internet of Things has skyrocketed. One example is the pervasiveness of mobile phones in modern life. The popularity of web-based assaults has skyrocketed with the exponential the expansion of online user populations. Now, security companies are attempting to combat these online assaults. Unfortunately, new forms of these assaults are appearing all the time, making it hard for older security measures to stay up. In computing, AI refers to a source of optimism in the current cybersecurity landscape, offering a potential solution to the ever-changing digital dangers. The fact that artificial intelligence has grown exponentially over the last decade and is now impacting the development of every other industry is the source of this optimism. With AI bringing so many advantages in every field, online security is one sector that just cannot afford to ignore it. The research presented in this thesis represents an advance in that path. This thesis details an effort to use AI to address serious issues with online security.

Keywords: Social Networking, web-based, industry, websites, revolutionized

Introduction

The term "social networking" refers to a broad category of online services that enable users to create limited-access or fully public profiles. In addition, it is usual practice for many SNSs to enable users to exchange private messages and leave permanent comments on profiles. Social networking sites, in example, are either organised or personal networks, depending on the preference of the user. Instead of limited social networking features like sharing digital pictures and videos, many SNSs like Four social networking sites: Friendster (2002), LinkedIn, Myspace (2003), and Facebook (2004) offer a number of features for teamwork, including user profiles and friendly connections, file sharing, discussion participation, and even start blogs. Orkut (2005), Bebo (2005), and QQ are a few more popular social networking websites that have recently emerged (2006). The introduction of mobile phones into social networking was a game-changer with the 2006 launch of Twitter. The services offered by various social networking websites throughout the globe are being heavily used by Indians who utilize the internet. How Orkut became popular in India popularised the use of social networking websites, but in modern times, these sites have become a cultural phenomenon. Everyone from tech-savvy urbanites to high school students has an account on a social networking website and makes heavy use of all the features. Every single person in India who has access to the internet has an account on at least one of these social media platforms, as it turns out. One million plus individuals have signed up for Rediff.com's social networking version since it began not long ago; this is just one of several local Indian social networking websites vying for attention. A lot of people in

India utilise social media sites like Minglebox, Hi5, Yaari, and a few more.

Literature Review

Mavani and Asawa (2017) [3] conducted research on the viability of spoofing attacks on 6LoWPAN networks. The two types of attacks that exhibited behaviour similar to IPv6 addresses with the MAC address have been identified. Both of these criminals attacked the data of the unprotected wireless network by following the same path as 6LoWPAN. Using the characteristics analysed by the radio propagation system, we may assess the attacker's success rate. It turns out that the loss of signal route is a major factor in the attacker's success rate. The network was simulated in the Cooja simulator and tree model has been used for attacker detection. By calculating the route loss distance and loss of distance exponents, the findings demonstrate that the attacker's success rate has been examined.

As a security measure for 5G wireless networks, an intrusion detection system depends on spoof Gupta et al. first proposed detection. (2017). The bandwidth of a spoofing assault has been studied using game theory. Any situation in which two entities or objects interact in accordance with the rules of a game may be analysed using game theory. Theoretically, there is a fixed number of movements that the client can make in the game. The strategy that an attacker uses to win the game via bandwidth fraud has been analysed using game theory in this article. Both the attacker and the relayor client are involved in the exchanges described here. Each uses the game to get access to bandwidth.

(2018) van der Stratified spoofing assaults into a classification system. Because of this, we can evaluate potential threats and countermeasures used by operational spoofers. Application, control policy, handover policy, and deployment architectures make up the layered model. This article delves further into the buyer's position management rules, drawing attention to operational challenges and offering solutions. This highlights the need of controlling the intended receiver, even after the signal has been successfully falsified. Furthermore, anti-fraud strategies and the most probable fraudulent assaults have been detailed.

A method to prevent IP spoofing was introduced by Singh et al. (2019) [2] utilising Artificial Bee Colony (ABC) and ANN as ML approaches. After optimising the nodes' attributes using ABC, ANN learns them and stores them in its database. The MATLAB program was used to conduct the simulation.

Using the idea of ML, Ajiginni (2020) [1] has created a method for detecting IP spoofing MItMA in wireless networks. We used the FFNN (Feed Forward Neural Network) method to construct the model. in the Python 3.6 toolbox. It was Kaggle that provided the dataset. Data that has been filtered and the properties that are sought have undergone pre-processing. A number of features have been chosen, including "duration," "protocol type," "service," "src_bytes," "flag," "land," "wrong fragment," "urgent," "hot," and so on. According to the findings, the current technique outperformed the prior methodology in identifying MItMA IP spoofing.

Research Methodology

History of Social Networking

People of all ages, from teens to adults, may benefit from the proliferation of online social platforms that enable them to connect with others online. By expanding their online networks via the social media platform, users of all ages and walks of life have been able to enrich their online experiences. Originating in Bulletin Board Service (BBS) technology, social networking has since progressed. Next, BBS is integrated with services like as email, chat, and voice chat to create the idea of social networking. Classmate, a website that allowed users to find friends online, see what they were up to, and interact with them, revolutionized social networking in 1995.

International Status

The popularity and growth of Social Networking Sites all over the world highlights how both national and local cultures decide the impact of technology those are commonly available between countries through activities carried out on Social Networking Sites by their users.

National Status

Table 1: Five Most Popular International Social Network Sites

Sr. No	USA	UK	South Africa	Thailand	India
1	Facebook	Facebook	Facebook	Hi5	Facebook
2	MySpace	Bebo	Youtube	Facebook	Twitter
3	Classmate	YouTube	Blogger	Wikipedia	Instagram
4	AOL	Myspace	Gumtree	Youtube	Hi5
5	LinkedIn	Blogger	Flikr	Myspace	Yaari

Online Social Media Platforms

Online social communities provide different services. They provide facility to communicate with friends, family, peers and other people having interests in same topics. Other services on social networking sites include downloading of information, sharing information including digital photograph and video. The most popular service provided via online social media facility to communicate the ability to build one's own network and become visible to others, facilitating interactions with strangers. People on this network will be able to interact with one another and have regular conversations, with the possibility that some of them may even employ offline modes of communication. On most social media platforms, users are more interested in chatting with individuals they already know and are already a part of their lives than in meeting new people. existing network.

Fig 1: Facebook Profile Page

Users of the microblogging service Twitter are able to share updates using only 140 characters: Twitter closely resembles Facebook in appearance and functionality; however, it is far more stripped-down and intended for brief remarks and picture postings instead of lengthy status updates. Additionally, the focus is more on followers than friends. If you want to keep your followers up-to-date on your latest comments (called tweets), you may do that by posting them to your Twitter feed. Other people's tweets may be followed by you if you choose to. You may expect your Twitter page to be updated whenever they tweet. Anyone can follow you, and you can follow anyone. To keep up with your favorite politicians and celebrities, follow their Twitter accounts. Some of your loved ones may even be active on Twitter. Despite the ability to attach images to tweets, the famous 140-character restriction on individual tweets forces you to stay succinct.

Fig 2: Twitter feed

YouTube: Ranks first among all video sharing websites. A YouTube channel is a great way for departments that have a videographer or produce a lot of films to share them with the world. The most popular video sharing platform in the globe, according to Sha, is YouTube. After then, site visitors may see the videos on their browsers. The sheer number of videos available on YouTube is in the millions. You can check which videos are currently trending (popular) by navigating to the left-hand side of the screen, and it also has a rating system where users may like and promote videos.

Fig 3: YouTube Video

Results

The aim of the chapter is to report the outcome of the data analysis which transformed the raw data, obtained from the study, into meaningful facts. The data presented in this chapter is obtained from close ended questionnaire collected from the sampling among total population of social networking users from Kolhapur and Sangli district in order to evaluate users' attitude and intention towards Social Networking and investigate their concern about privacy and safety.

Data Analysis and Interpretation

This research intends to analyze different security and privacy issues associated with Social Networking web sites. Hence sampling is limited to participants with knowledge and skill about using Social Networks.

Table 2: Sample Profile

Particulars		Male	Female	Total	
Student	UG Student	120	88	208	250
	PG Student	24	18	42	
Non- students	Businessman/Self-employed	9	4	13	250
	Employee	97	61	158	
	House Wife	0	79	79	
	Total	250	250	N=500	

Table 3: Tools used to access social media

Sr.	Particulars	Respondents		Percentage
1	pc	217	143	29
2	Mobile	383	252	50
3	Laptop	149	98	20
4	Other	11	7	1
Total		760	500	100

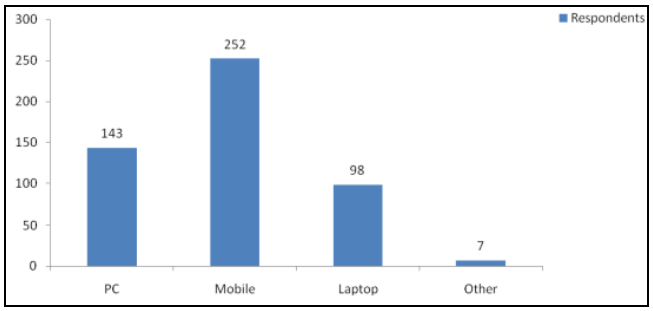

Fig 4: Tools used to access Social Networking Sites

Test Used: Kolmogorov-Smirnov Test

Table 4: Opinion for decrease in e-mail use.

Sr.	Particulars	Respondents
1	Strongly Disagree	5
2	Disagree	5
3	Neutral	3
4	Agree	15
5	Strongly Agree	472
	Total	500

Application of the Chi-square test

Table 5: Details of time spending on Social Networking Site

Sr.	Particulars	Respondents	Percentage
1	0-10hrs	85	17
2	11-20hrs	50	10
3	21-30hrs	98	20
4	31-40hrs	255	51
5	40hrs+	12	2
Total		500	100

Conclusion

When asked about their knowledge of smartphones, respondents were usually competent. while making new friends through social networking sites. Majority of social networking users surveyed have joined the social networking due to the popularity it has created through news but at the same time less concerned about security and privacy issues like Geotagging. Although social networking companies are giving improved facilities in order to handle privacy and security concerns, the usage agreements indicate that most responsibility lies at users‟ side. In order to safeguard themselves against cybercrime, users should keep up with the latest advancements in the realm of social media and mobile technology, particularly as they pertain to information security. That will keep children secure from dangers is a major worry amongstit users.

References

1. Ajiginni AD. Identification and Classification of IP Spoofing Man in the Middle Attack using Multilayer Perceptrons [Doctoral dissertation]. Dublin: National College of Ireland; c2020.
2. Singh R, Thakur K, Singh G, Gupta S. Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network. In: Proceedings of the Third International Conference on Advanced Informatics for Computing Research. 2019. p. 1–10.
3. Mavani M, Asawa K. Modeling and analyses of IP spoofing attack in 6LoWPAN network. Computers & Security. 2017;70:95–110.
4. Gupta A, Jha RK, Gandotra P, Jain S. Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network. IEEE Transactions on Vehicular Technology. 2017;67(1):618–632.
5. van der Merwe JR, Zubizarreta X, Lukčin I, Rügamer A, Felber W. Classification of spoofing attack types. In: 2018 European Navigation Conference (ENC). IEEE; c2018. p. 91–99.
6. Singh R, Thakur K, Singh G, Gupta S. Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network. In: Proceedings of the Third International Conference on Advanced Informatics for Computing Research; c2019. p. 1–10.
7. Dong P, Du X, Zhang H, Xu T. A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In: 2016 IEEE International Conference on Communications (ICC). IEEE; c2016. p. 1–6.
8. Jaber AN, Rehman SU. FCM–SVM based intrusion detection system for cloud computing environment. Cluster Computing; c2020. p. 1–11.
9. Diro AA, Chilamkurti N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems. 2018;82:761–768.
10. Jadhav BN, Gupta HK. A Modified Algorithm and Protocol for Replica Attack Prevention for Wireless Sensor Network. International Journal of Technology Research and Management. 2020;7(1):1–5.