DETECTION OF PHISHING WEBSITES USING MACHINE LEARNING

[1]Pathare Ujjwala Balasaheb, [2]Lokhande Gayatri Digambar, [3]Machale Manjushri Suresh, [4]Gunjal Kajal Dattatrya, [5]Prof. Gunaware Nilesh Genaba

HSBPVT's Parikrama group of institutions, Kashti , Ahmadnagar

Ujjwalapathare12@gmail.com[1], Gayatrilokhande85@gmail.com[2], Manjushrimachale2001@gmail.com[3], Gunjalkajal522@gmail.com[4]

ABSTRACT

We know that the mobile devices have become so common, there is a trend toward moving practically all offline activity online. The simplest method for obtaining sensitive information from unwitting users is through phishing attacks. Phishers seek to get private data, including usernames, passwords, and bank account details. Cybersecurity experts are searching for consistent and dependable methods of detecting phishing websites. In this research, numerous properties of both genuine and phishing URLs are extracted and analyzed in order to detect phishing URLs. Phishing websites can be recognized using decision trees, random forests, and support vector machine algorithms. The results demonstrate the effectiveness of machine learning in proactively identifying phishing websites, thereby enhancing cybersecurity measures.

learning, contributing to the overall improvement of online security and privacy.

INTRODUCTION

Detecting Phishing Website Using Machine Learning Project in PYTHON is a web-based technology that detect fraud websites. Phishing attacks, a type of cyber threat, have become increasingly prevalent and sophisticated in the digital age. Phishing involves deceptive attempts to trick individuals into disclosing sensitive information, such as login credentials, financial data, or personal details. These attacks often manifest in the form of fraudulent emails, fake websites, or social engineering tactics. Phishing can have severe consequences, including financial losses, identity theft, data breaches, and reputational damage Phishing is a fraudulent technique that uses social and technological tricks to steal customer identification and financial credentials. Social media systems use spoofed e-mails from legitimate companies and agencies to enable users to use fake websites to divulge financial details like usernames and passwords . Moreover, Most phishing attacks target financial/payment institutions and webmail, according to the Anti-Phishing Working Group (APWG) latest Phishing pattern studies .

LITERATURE SURVEY

1.Phishing Detection Using Machine Learning Technique

Authors: J. Rashid, T. Mahmood, M. W. Nisar and T. Nazir

This paper proposes an approach of phishing detection system to detect blacklisted URL also known as phishing websites, so that individual can be alerted while browsing or accessing a particular website. Therefore, it can be utilized for identification and authentication and become a legitimate tool to prevent an individual from getting tricked. The system fosters many features in comparison of other software. Its unique features such as capturing blacklisted URL's from the browser directly to verify the validity of the website, notifying user on blacklisted websites while they are trying to access through popup, and also notifying through email. This system will assist user to be alert when they are trying to access a blacklisted website.

Remarks: Used different approaches rather than machine learning. According to the survey ML is more effective than the other approaches.

2)Phishing Detection Using Machine Learning Technique

Authors: J. Rashid, T. Mahmood, M. W. Nisar and T. Nazir

This paper proposes an approach of phishing detection system to detect blacklisted URL also known as phishing websites, so that individual can be alerted while browsing or accessing a particular website. Therefore, it can be utilized for identification and authentication and become a legitimate tool to prevent an individual from getting tricked. The system fosters many features in comparison of other software. Its unique features such as capturing blacklisted URL's from the browser directly to verify the validity of the website, notifying user on blacklisted websites while they are trying to access through popup, and also notifying through email. This system will assist user to be alert when they are trying to access a blacklisted website.

Remarks: Used different approaches rather than machine learning. According to the survey ML is more effective than the other approaches.

3)Detection of Phishing Websites Using Machine Learning

Authors: A. Razaque , M. B. H. Frej, D. Sabyrov, A. Shaikhyn, F. Amsaad and A. Oun

In this paper, we contribute to solving the phishing problem by developing an extension for the Google Chrome web browser. In the development of this feature, we used JavaScript PL. To be able to identify and prevent the fishing attack, a combination of Blacklisting and semantic analysis methods was used. Furthermore, a database for phishing sites is generated, and the text, links, images, and other data on-site are analyzed for pattern recognition. Finally, our proposed solution was tested and compared to existing approaches. The results validate that our proposed method is capable of handling the phishing issue substantially.

Remarks: Focused on all the features rather than the important features this makes to increase time complexity.

Future Scope:

1. User Protection
2. Email Security
3. Fraud Detection
4. Open Source Projects

CONCLUSION:

It is found that phishing attacks is very crucial and it is important for us to get a mechanism to detect it. At present generation attackers are more in network ,phishing has become major security problem ,causing many losses by hacking he legal data that are used by the user through this project, one can know a lot about the phishing websites and how they are differentiated from legitimate ones. These should classify the inputted URL to legitimate or phishing with the use of the saved model.

REFERENCE

[1] https://www.slideshare.net/ummeayesha/phishing-detection

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8504731/

[3] https://search.yahoo.com/search?fr=mcafee&type=E210US885G0&p=mathmatical+model+of+detection+of+phishing+website+using+machine+learning

[4] https://www.researchgate.net/publication/327340841_Detection_and_Prevention_of_Phishing_Attack_Using_Linkguard_Algorithm