DETECTING PHISHING WEBSITE USING MACHINE LEARNING

Dr. R.S. Apare, Suraj Rakesh Gupta, Shivam Kumar, Manmit Sian, Jugal Dave

SKNSITS,Lonawala

ABSTRACT:

Phishing is a crime involving robbery of confidential userdata. The phishing websites are aimed at individuals, businesses, and cloud storage and government websites. Hardware- based anti- phishing methods are generally used, but software- based approaches are favored because of costs and operational factors. There is no solution to the problem such as zero- day phishing attacks from current phishing detection approaches.

Keywords: *Deep learning, RecurrentNeural Network, Attack Detection.*

INTRODUCTION

Phishing is a type of cybercrime in which a personimpersonating a legitimate organisation contacts a victim or target via email, phone, or text message to entice them to provide personal information, banking and credit card information, and passwords. Phishing is a serious offence. The newterm 'fishing' refers to an attacker's invitation to visit a fake site by imitating a website's appearance in order to obtain personal informationfrom users such as usernames, passwords, financial information, account details, national security identifiers, and so on. Phishing is a new phrase coined from the word 'fishing.' The data gathered is utilised for prospective target advertisements or potentially identity theft and attacks (such as money transfers from one's account). Sending e-mails, messages that can leadto data theft or personal information, is a commonattack strategy.

OBJECTIVE

- Aim is to develop application for peoples whomake our nation more digital and scam free through an online banking.
- The objective of the proposed system is to provide best possible security mechanism to provide confidence to the people make most oftransaction online.
- The objective behind this system is to invent a system widely acceptable for providing vital role in security concern for banking era.
- We have to provide perfect approach for online banking with the help of anomaly-based detection and prevention of phishing attacks.

REQUIREMENT SPECIFICATION

Hardware Requirements

- Processor - Intel i3/i5/i7
- Speed - 3.1 GHz
- RAM - 4 GB s(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor – SVGA

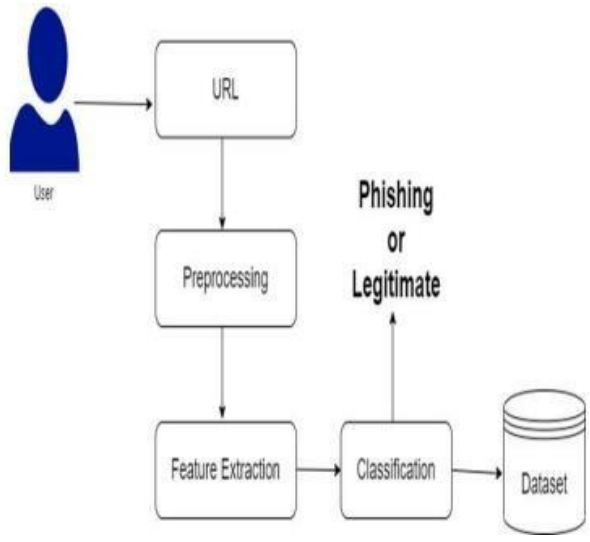
Software Requirements

Operating System - Windows

- Application Server - Apache Tomcat
- Front End - HTML, CSS, Bootstrap
- Language - Java.
- Database - My SQL
- IDE - Eclipse

METHODOLOGY

Architecture Diagram

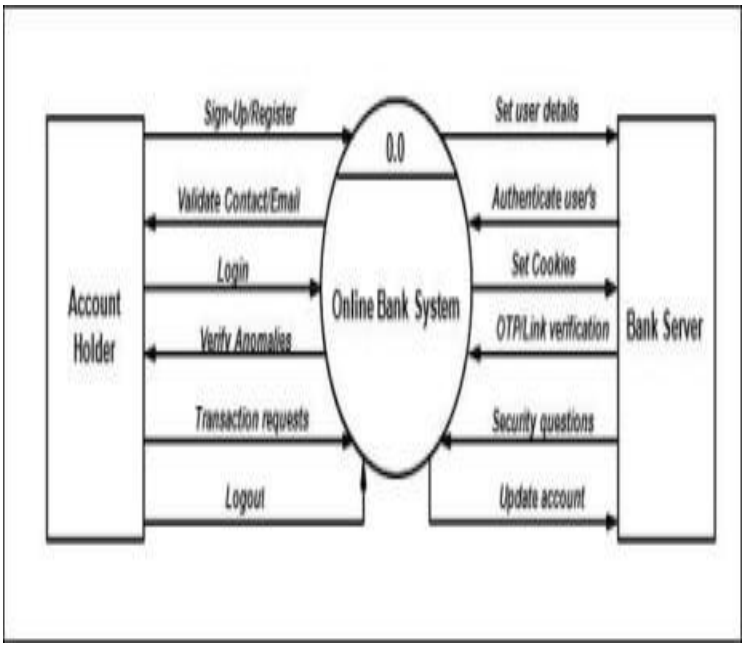


Mathematical Model

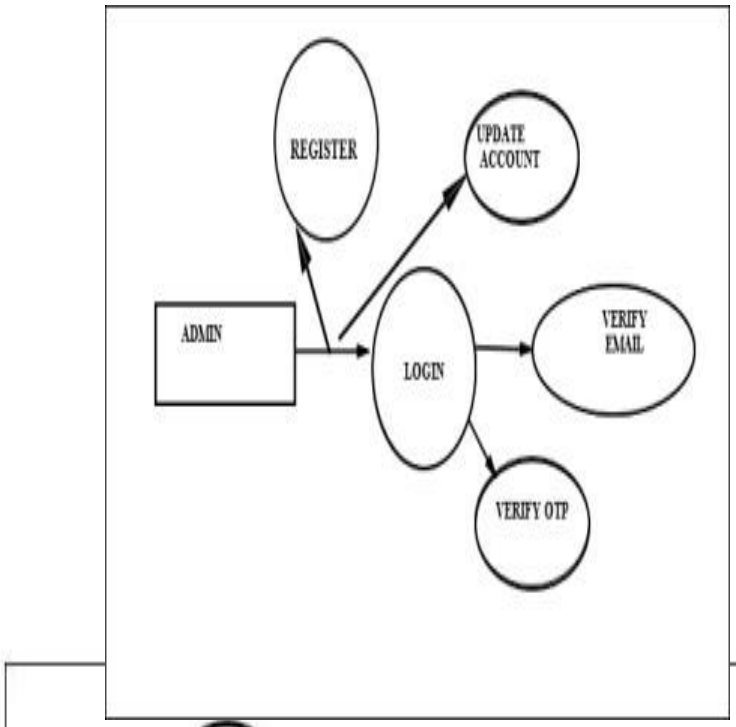
Let us consider S as a Phishing Websites Detection. S= { } INPUT: Identify the inputs as URLS. F= f1, f2, f3.....,fn— 'F' as set of functions
I= i1, i2, i3.....'I' sets of inputs to the function
set O= o1, o2, o3.....'O' Set of outputs from the
function sets S= I, F, O I = URL O = Secure or notF = Fetch data, data preprocess, classification

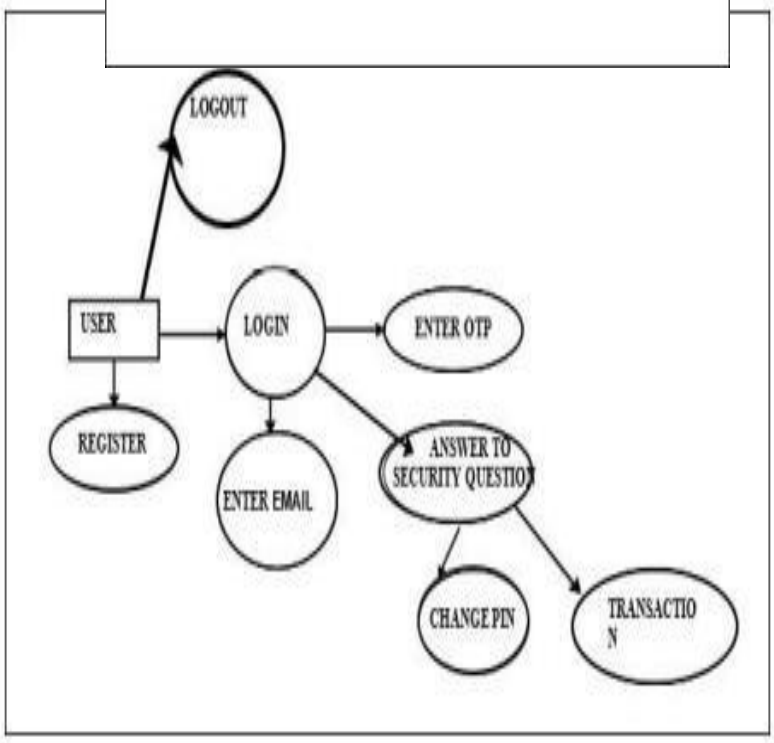
DFD

Level-0 DFD



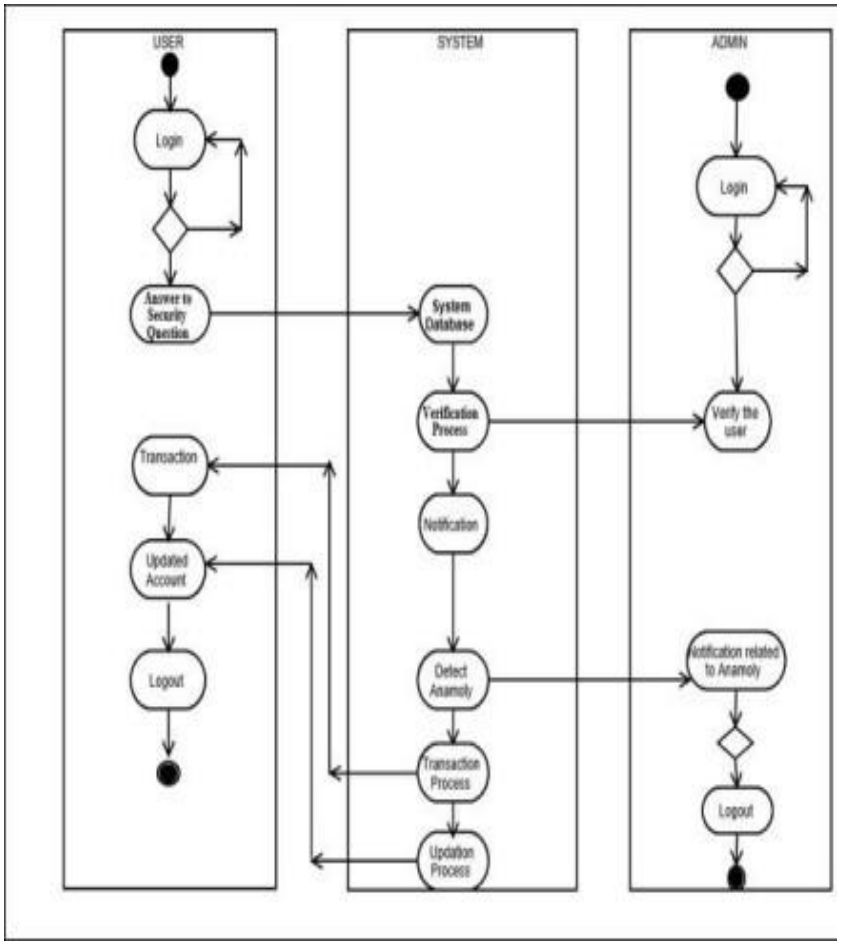
Level-1 DFD





Level-2 DFD

Activity Diagram



CONCLUSION

Phishing is one of the most devastating types ofweb security risks available today. According toour research, we have developed a prediction model for the identification of Phishing websites,which is based on an analysis of the attributes of the attack. The deep recurrent neural network's deepseated learning model outperforms other machine learning models in terms of prediction and achieves the highest level of precision.

REFERENCES

[1] Surbhi Gupta et al., "A Literature Survey on Social Engineering Attacks: Phishing Attack," in International Conference on Computing, Communication and Automation (ICCCA2016), 2017, pp. 537-540.

[2] Jian Mao, Wenqian Tian, Pei Li, Tao Wei, Zhenkai Liang, "Phishing Alarm: Robust and Efficient Phishing Detection via Page ComponentSimilarity".

[3] Zou Futai, Gang Yuxiang, Pei Bei, Pan Li, Li Linsen, "Web Phishing Detection Based on Graph Mining", Guardian Analytics, "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security". Accessed: 08 Jan 2018.

[4] Ibrahim Waziri Jr., "Website Forgery: Understanding Phishing Attacks Nontechnical Countermeasures," in IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015, IEEE.

[5] LongfeiWu et al,"Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE 2016, pp. 6678-6691.

[6] K. Rajitha and D. Vijayalakshmi, "Suspicious URLs filtering using optimal rtpfl: A novel featureselection based web URL detection," in Smart Computing and Informatics, S. C. Satapathy, V. Bhateja, and S. Das, Eds. Singapore: Springer Singapore, 2018, pp. 227–235.

[7] S. Kim, J. Kim, and B. B. Kang, "Malicious url protection based on attackers' habitual behavioral analysis," Computers Security, vol. 77, pp. 790 – 806, 2018.