

Cyber Security and Artificial Intelligence

Dr. Abdul Mateen Ahmed¹, Mohammed Shahbaz², Raveeya Zareen³, Syed Mujeeb UHassan⁴,
Mohammed Abdul Sami Uddin⁵, Mohd Viqar Ullah Kaif⁶ and Mohammed Aman uddin⁷

¹⁻³ISL Engineering College/Department of ECE,Hyderabad, India

Email: abdulmateen@islec.edu.in, shahbazmohammed2000@gmail.com, raviyazareen22@gmail.com

⁴⁻⁷ISL Engineering College/Department of IT,Hyderabad, India

Email: syedmujeebul@gmail.com, mohammadabdulsami6187@gmail.com, mohammedviqar7@gmail.com,
amanuddin4@gmail.com

Abstract—Cyber security plays an important role in the field of information technology. Privacy and security of the data will always be the top security measures that any organization takes care of with the digitalization of India. The Internet has reached every corner of the country whether it is in urban and rural areas. Social media, online shopping, money transfer everything is only a click away Cyber threats are also increasing with the rising number of Internet users. The main reason rural people get victimized by cyber attacks is lack of awareness about these issues. The concept of username and password have been fundamental way of protecting our information. The OTP feature prevents some forms of identity theft by making sure that a captured password cannot be used a second time. Encryption is the process of encoding messages and information in such a way that eavesdroppers or hackers cannot read it. In encryption schemes, the personal and confidential information such as transactions, emails, bank account details etc. are encrypted using an encryption algorithm turning it into an unreadable ciphertext.

Cyber security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. There is no perfect solution for cyber crimes but we should try our level best to minimize them. This paper mainly focuses on challenges faced by cyber security in rural areas. It also focuses on cyber security techniques, cyber crime and social media.

Index Terms— Cyber security, Artificial Intelligence, Rural Development, Wireless Network, Cyber threats.

I. INTRODUCTION

This research is about the awareness of cyber security in the rural community. The present days, the application of the internet suddenly increased, which is the cause of network trafficking[1]. That increases risk of cyber crime for the local authority, employees, since they are supposed to use their devices to access their accounts[2]. This research is conducted with the objective to raise awareness and educate the rural community about the importance of cyber security[3]. The rural communities have been ignored in being given an education about cyber security. In another research we come to know that the rural community nor has any awareness in cyber security. The role of local authority is important to provide awareness in cyber security. Cybercrime targeted rural communities where most are individual in nature and rarely hear about these cases in the national media[4]. The material for teaching rural communities should be easy to understand so the local authority can be

understood.

In research we take a person “MIC” in consideration who starts doing online shopping[5]. He got a “Gift voucher” message from the fake account of shopping.com ,he filled all the bank account details with the thought that it's a formality. Because of this mistake all of his bank details got corrupt. There a question a rais “ can he prevent this attack? The answer is yes he could prevent these attacks if he had the knowledge about cyber crime and cyber security[6].

A. Types of cyber attack[7-10]

- 1)Malware attack:-due suspicious messages which are downloaded from online,spy etc.
- 2)Phishing attack:-by fragel emails which look like from a legitimate source.
- 3)Man-in-middle attack:-here the hacker gain the access to the information path between mic device and the website server hacker takes over mic ip address by doing so the communication line between our device and the network secretly interrupted ,this commonly happen with unsecure wifi network and also through malware
- 4>Password attack:-it's a one of the easy ways to hack the system here the mic password could be cracked by the common password or try all alphabetic possible passwords.

B. How to prevent feature cyber attack[11-13]

We can implement some cyber security practices

- 1)Firewalls :-its a virtual wall that filters the incoming and outgoing traffic from your device to guard the network.
- 2)Honeypot:-just like flowers attract bees,damey computers called honeypots are used to attract hackers. This system is made to look vulnerable to decisive attackers and this in turn protects the real system. In addition to this we can also use a unique alphanumeric password and antivirus software which avoid the mails from unknown devices[14-20].

II. SYSTEM MODEL

The basic system model as shown in the figure deploys the technical aspects of a Secured network connections proposed

- However, now-a-days wifi router most widely used device in a day to day life.
- Wifi router is mostly targeted by the cybercriminals to steal the user's any private and sensitive Information.
- To secure wireless networks like wifi router and any there access at homes and any of Companies,We a normal person doesn't need any type of Cybersecurity experts,or we don't have pay a lot of Money to secure our Devices,to secure our Private Data.
- We, people can also Secure our Devices with taking some measures or by doing or using some Techniques.
- To Implement simple Techniques, We can Enhanced Security in Internet Home Devices.

III. RESULTS

The research conducted by the authors confirms that this lack of awareness, combined with the deep-rooted dangers posed by the internet, expose local communities to cyber threats. Enhancement of security and Privacy Policy connected to wireless networks is done.

Online Google Forms was designed to identify user impacts due to wireless network related attacks in the remote areas and in particular to Village. The targets were both technical and non-technical based users which consists of a random 56 sample.The survey uses a quantitative technique using online questionnaires. We asked our target users if they faced any kind of cyber attack during the pandemic (quarantine time), and what kind of attack/threat they experienced and how they dealt with it. We provided options of common wireless related attacks to choose from such:

1. Your password was not working, but you are very sure it was correct
2. You were not able to access to the website that you need; it was always down
3. You were purchasing something online and suddenly your current page redirected to another page
4. Someone came from TeleCom/STC offering you to increase your Wifi band for free
5. Someone called telling you win 1000\$ and share your banking details
6. You were buying something online, and website asked you to provide sensitive information; social ID, username & password

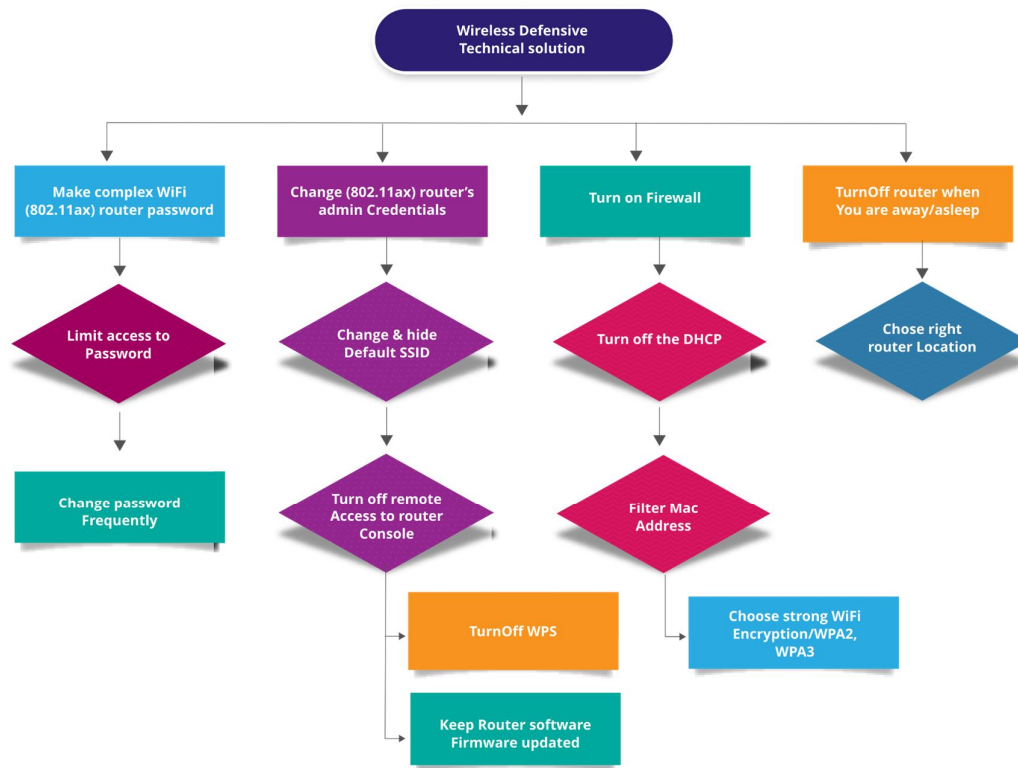


Fig 1. Wireless Network Security Enhancement figure(i)

You saw someone in your neighborhood in the car using a laptop with some weird antennas Survey results as follows; most people (66.7%) faced phishing attacks because ‘Someone called telling you win 1000\$ and share your banking details’, (42.9%) of people experienced DoS attack, ‘You were not able to access to the website that you need; it is always down’, (33.3%) of people experienced social engineering attack ‘You were buying something online, and website asked you to provide sensitive information; social ID, username & password’. We also asked questions to identify how people mitigate or dealt with attacks that they were experienced, where most of people (62.5%) ‘Did nothing’ when they actually were attacked, because people cannot easily differentiate phishing/fake emails, malware websites, social engineering masquerading tricks. Thus, users should be aware and take simple precautions to stay protected as well as enhance their security and privacy issues while using wireless networks.

IV. CONCLUSIONS

These themes are developed in such a way to cover a wide range of topics, including practical advice on phishing attack avoidance and more advanced topics such as preventing social engineering attacks. This paper will introduce the development of the cyber security awareness program, and bring the importance for including these specific themes at the hand of international cyber security incidents.

This research paper focuses on promoting cyber security awareness towards the newly released broadband capability and knowledge transfer within rural communities by means of an optional community based training program. This program can be adapted in any environment other than rural areas, but the current focus has been in the rural areas.

ACKNOWLEDGMENT

The authors wish to thanks Principal Dr. Mohammed Masood, Chairman Mr. Mohammed Salman , HoDs and Faculties of the ISL Engineering College. This work was supported in part by a grant from ISLEC.

REFERENCES

- [1] Annette B, Thomas G and Julius K, "Emotion and Intuition: Effects of Positive and Negative Mood on Implicit Judgments of Semantic Coherence", *Psychological Science*, Vol.4, Issue.5, pp:416-421,2003.
- [2] Crowder, J.A., Friess, S., "Artificial Neural Diagnostics and Prognostics: Self-Soothing in Cognitive Systems." *International Conference on Artificial Intelligence, ICAI 10* , July 2010.
- [3] Crowder, J. A., Friess, S., "Artificial Neural Emotions and Emotional Memory" *International Conference on Artificial Intelligence (ICAI 10)* ,July 2010.
- [4] Crowder, J. A., "Flexible Object Architectures for Hybrid Neural Processing Systems." *International Conference on Artificial Intelligence, ICAI 10*, 2010.
- [5] Marsella, S., and Gratch J., "A Step Towards Irrationality: Using Emotion to Change Belief." *1st International Joint Conference on Autonomous Agents and Multi-Agent Systems*, Bologna, Italy, 2002.
- [6] Miller E.K, Freedman D.J, Wallis J.D, "The prefrontal cortex: categories, concepts and cognition". *Philos. Trans. R. Soc. Lond. B, Biol. Sci.* 357 (1424): 1123–36, 2002.
- [7] J. Cheng, G.Y. Liu, "Research Progress on emotion recognition from the perspective of subject cross, *Comput. Sci.*" 39 (5) ,pp.19-24, 2012.
- [8] L. Lu, "A study of the multimodal cognition and interaction based on touch, audition and vision, *J. Comput. Aided Des. Comput. Graph.*" 4 (26), 2014.
- [9] M.H. Yang, "Nature multimodal human-computer-interaction dialog system, *Comput. Sci.*" 10 (41), pp-12-35, 2014.
- [10] Y.C. Huang, K.Y. Wu, Y.T. Liu, "Future home design: an emotional communication channel approach to smart space, *Personal Ubiquitous Comput.*", 17(6), pp.-1281-1293, 2013.
- [11] De Mello FL and De Souza SA, "Psychotherapy and Artificial Intelligence: A Proposal for Alignment",. *Front. Psychol.* 10:263. doi: 10.3389/fpsyg.2019.00263, 2019.2
- [12] Eysenck, M. W and keane M, "Cognitive psychology: A student's hand book", Psychology press, 2015.
- [13] Fiske A, Henningsen P, Buy X A, "Your Robot Therapist Will See You Now: Ethical Implications of Embodied Artificial Intelligence in Psychiatry, Psychology, and Psychotherapy", *J Med Internet Res*, 21(5):e13216, 2019.
- [14] Bostrom, N. "AI set to exceed human brain power. *CNN science and space*", 2006.
- [15] Gibney, E, "Google secretly tested AI bot with human psychology", 2017.
- [16] Crowder.J. "Robot therapist will see you know ethical implications of human psychology", 2019.
- [17] WegmanS, "Cognitive psychology and artificial intelligence theory and research in cognitive science",1984.
- [18] Tambe M and Newell. A, "Theory of human and artificial cognition Research", 1988.
- [19] Malik, "Dictionary Of Cognitive Psychology And Human Era",2011.
- [20] Terry D, "Artificial intelligence and creativity-an interdisciplinary approach", 2019.