IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 4 Ver. I (Jul. – Aug. 2017), PP 67-74
www.iosrjournals.org

Wi-Fi Adoption And Security Survey

*[1]Alimul Haque, [2]Nidhi Raj, [3]Anil Kumar Sinha and [4]N. K. Singh
[1,4]University Department of Physics, V. K. S. University, Ara 802301 Bihar, India
[2]B.Tech.(VI-Sem), Department of Computer Science & Engineering, S.B.M. Jain College of Engineering, Jain University, Bangalore-560004, India.
[3]Department of Computer Science, V.K.S.University,Ara-802301, India
Corresponding Author: Alimul Haque

Abstract: *The role of computers and the Internet in modern society is well recognized. Wi-Fi internet connection have become increasingly popular, it can become the spring board for rapid economic growth in the rural areas but the rapid growth of Wi-Fi access has also contributed to unethical practices by individuals who are bent on using the technology to exploit others. Such exploitation of Wi-Fi network for the purpose of accessing unauthorized or secure information, spying, disabling of networks and stealing both data and money is termed as Wi-Fi threats. Such attacks have been increasing in number and complexity since last few years. Hence there is a need to have comprehensive understanding of Wi-Fi threats. For keeping in view of Wi-Fi adoption and Security I am conducting a survey in old Shahabad (i.e. Bhojpur, Buxar, Rohtas and Kaimur).*

This survey report, investigates Wi-Fi usage, Wi-Fi accessibility, Wi-Fi security and the knowledge of it in old Shahabad. Data collected from the research shall help service provider to understand more about the user experience, awareness and perceptions of Wi-Fi service and security in Shahabad. Recommendations are given for deploying, managing and improving the wireless services in various sectors.

Key words: *Wi-Fi, wireless services, wireless networking, security*

Date of Submission: 19-06-2017 Date of acceptance: 22-07-2017

I. Introduction

Actually, wireless networks become an essential tool of communication due to their flexibility, effectiveness and low cost [1]. Wireless Fidelity (Wi-Fi) Technology is one of the upcoming techniques in the internet world [2]. The working of Wi-Fi is based on transmission process [3]. The data is transferred in the form of radio signals, and then the device transmits these signals to antenna which is used for transferring of data. This antenna which is used for transmission purpose is connected with a wired LAN or DSL.

Wi-Fi is generally used for linking devices in wireless form. Figure1 shows that Wi-Fi Network attaches computers to one another in a better communicable way. It creates an invisible path between the internet and the wired network [4]. It works on the physical and the data link layer. Radio Frequency (RF) is used for transmitting data through air. This is most remarkable feature of the Wi-Fi technology. It also provides better data speeds. IEEE 802.11 is considered as a position of values moving elsewhere is known as Wireless Local Area Network (WLAN). This is also a type of network communication. Access Point (AP) is considered to be an important feature in the Wi-Fi network technology [5]. It has a radio transmitter as well as radio receiver, which are directly connected with the wired network or to the internet network. Wireless Access Point basically helps connecting with devices likes digital cameras, tablet computers and digital audio players, PCs, video-game comforts, smart phones, laptops etc. This Access Point (AP) takes a common achievement as a base station for the entire Wi-Fi network.

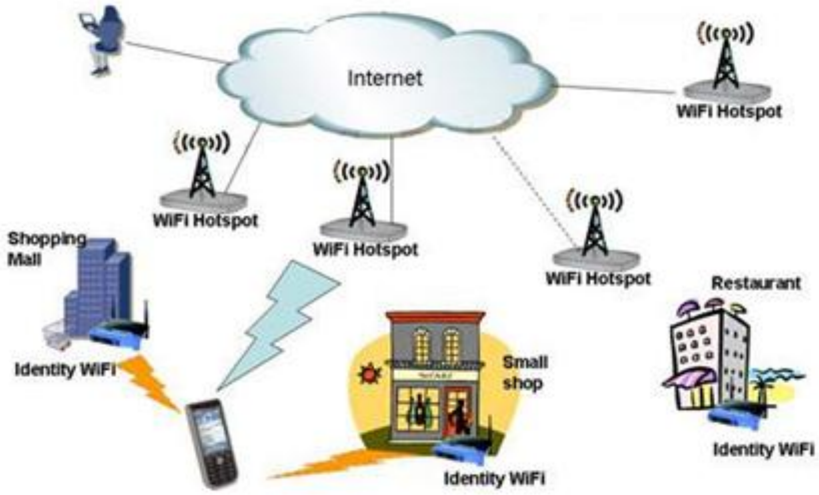


Figure1. Wi-Fi Internet Connection

The Wi-Fi network has been facing many security problems since its inception such as hacking and unauthorized access [6]. Wireless insecurity has been a critical issue since Wired Equivalent Privacy (WEP), an IEEE standard security algorithm for wireless networks, was compromised [1]. The hacker uses the wireless hacking tools like AirSnort, Aircrack, WepAttack, WEPCrack etc [7].

Sheldon, Weber, Yoo and Pan [8] explained how the Wi-Fi encryption standards such as WEP, WPA/WPA2 are vulnerable to attack. They described some of the attacks on encryption standards such as Chop-chop attack, Brute force, Beck-Tews, Halvorsen-Haugen and the hole 196 attacks etc. Wang, Srinivasan, and Bhattacharjee [9] presented a 3-way handshake model instead of the usual 4 way handshake method for the 802.11i protocol. They described how their alternative method can effectively prevent denial of service (DoS) attacks including de-authentication, disassociation and memory/CPU DoS attacks. Souppaya and Scarfone [11] presented the need for security concerns and these should be applied from the configuration design stage to implementation and evaluation through to the maintenance stage of the Wireless LAN. They also presented some general guidelines and recommendations in order to reduce the vulnerabilities and prevent the most common threats. Pan Feng [10] described that more than 70% of the wireless LAN security issues are due to human factors, such as data theft by acquaintances or colleagues. He presented that remaining 30% of security threats are system related. Reddy, Rijutha, Ramani, Ali, and Reddy [12] presented how WEP can be cracked by freely available open source software tools such as Netstumbler, Ministubler, Airopeek, Kismat, Cain etc. They have mainly focused on securing WLANs by realizing miscellaneous threats and vulnerabilities associated with 802.11 WLAN standards and have used ethical hacking to try to make these more secure. Li and Garuba [13] and Deng Shiyang [14] explain various encryption standards relating to 802.11 WLAN, their vulnerabilities and security flaws. Stimpson et al [15] discussed war driving techniques as a useful tool for assessing security and vulnerabilities of home wireless networks. However, none of the above researchers has elaborately explained Wireless LAN security vulnerabilities, threats and general guidelines/recommendations for securing them.

The common users don’t know the know how of the technology. They simply use it for their communication needs. Even they don’t bother about the security threats. They simply expect consistency and mobility from its. Service providers are aware of the expectations of their customers. They strive to satisfy the needs and their expectation of the customers.

This survey investigates Wi-Fi usage, accessibility to it, its security and awareness of the people of old Shahabad. Realizing the vulnerabilities, understanding the most common threats and providing general guidelines and recommendation in order to protect Wi-Fi network and make them more secure for the home user and for enterprise networks is the objective of this paper

Data collected from the research shall help service providers to understand more about the user’s experience, awareness and perceptions of Wi-Fi service and security threats in Shahabad.

By way of critical data analysis, it is hoped that findings of the research will assist both the government and commercial Wi-Fi network providers to identify the gaps between the current services and the future directions of its improvement.

II. Problem Statement

Due to the fact that there is scant research on security threat for Wi-Fi users in the districts of Rohtas, Kaimur, Buxar and Bhojpur of Bihar, there is a need to conduct such studies on periodical basis to assess users' satisfaction with Wi-Fi networking and security services.

III. Objective of the study

The main objectives of the study are to

- To explore the frequency and purpose of users of Wi-Fi networking in the districts of Buxar, Kaimur, Bhojpur & Rohtas of Bihar.
- Determine user's satisfaction with Wi-Fi networking services.
- Assess user's perception of security threat to Wi-Fi networking services.
- Identify the issues arising from security threats for Government sector as well as private sector.

IV. Research Methodology

The survey research method was used. Based on objectives of study, a close ended questionnaire was developed to collect the data needed. So issues its validity and reliability, the questionnaire was reviewed by several professor of Computer application and Physics. Their suggestions were incorporated accordingly. The population of the study includes educated students internet and mobile users and mostly studying at colleges and Veer Kunwar Singh University, Ara.

The total population of study constituted 300 participants, out whom a sample of 250 respondents was drawn. The random sampling technique was used by distributing an equal number of questionnaire copies among the subject s of the study. Out of a sample 250 participants 210 respondents respond through online Google form.

This research was focused on the following main research question: **"Perception of Wi-Fi security and threats"?** Based on the purpose of the research, the following questions arise.

1. What kind of participants are the users of Wi-Fi?
2. What are the purpose of using Wi-Fi?
3. How much times are spent on Wi-Fi connection?
4. At which places participants generally use their Wi-Fi connection?
5. What are the current challenges that participants perceive with Wi-Fi?
6. What kind of technique can be used to protect their Wi-Fi connection from hacker?
7. Is security enough to internet access through Wi-Fi hotspot?
8. Have participants ever experienced hacker attack or received virus in Wi-Fi connection?
9. Do the institution provide Wi-Fi security?

4.1 Research Method

The above questions were used to gather initial data, such as the general information about the use of Wi-Fi from individual participants. The participants enjoy freedom to give their replies. The primary data of this research was the one gathered from interviews. The strategies and procedures for data gathering are based on observation, survey, and interview.

V. Data

This section presents quantitative data results. As described in the previous section, all the participants were selected randomly from old Shahabad(i.e. Bhojpur, Buxar, Rohtas and Kaimur) of Bihar during January 2015 to June of 2016. The quantitative data was coded separately for appropriate comparisons and/or classifications in data analysis section.

5.1 Quantitative data findings

5.1.1. Surveys as in Figure[2]-[13]

*** Participants' residence profile**

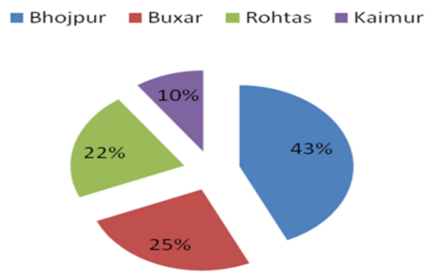


Figure.2 Residence profile of respondents

*** Experience profile of participants**

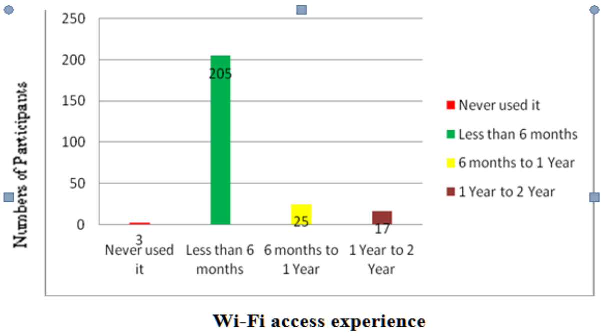


Figure.3 Participants Wi-Fi Experience

*** Use of Wi-Fi by Smartphone**

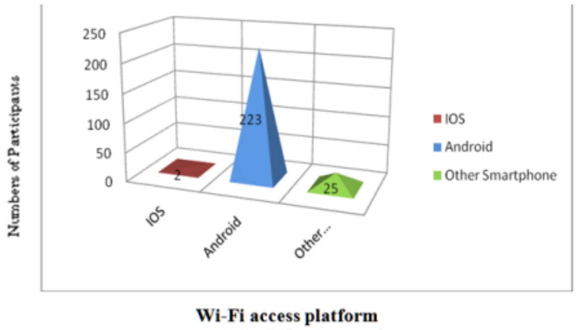


Figure.4 Wi-Fi by Smartphone

*** Activities conducted through Wi-Fi Network**

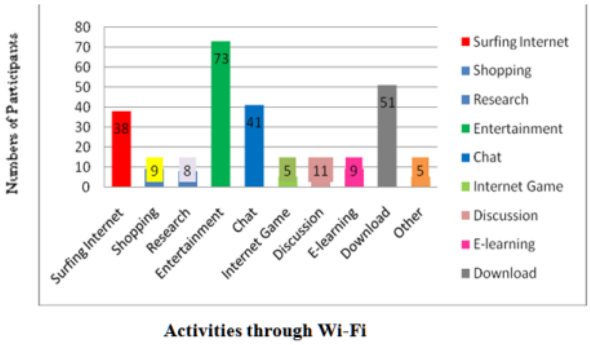


Figure.5 Purpose of using Wi-Fi connection

*** The duration of the use of Wi-Fi connection**

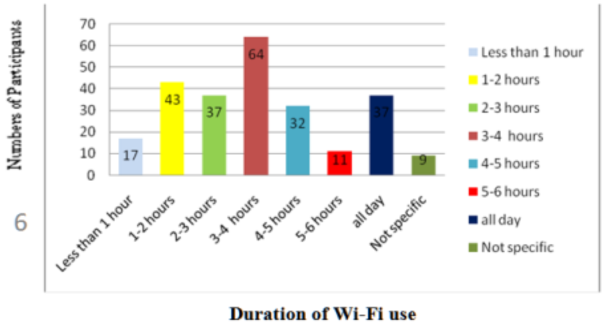


Figure 6 Time spend on Wi-Fi connection

*** Place where participants usually use the Wi-Fi**

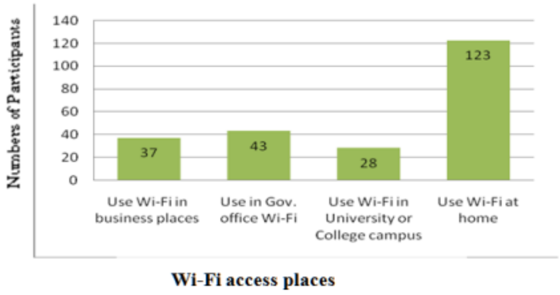


Figure.7 Place of Wi-Fi use

*** Security knowledge of Wi-Fi**

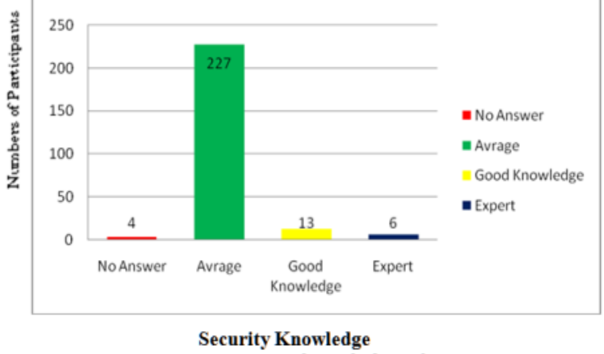


Figure 8. Security knowledge of Wi-Fi

*** Perception of Wi-Fi Security**

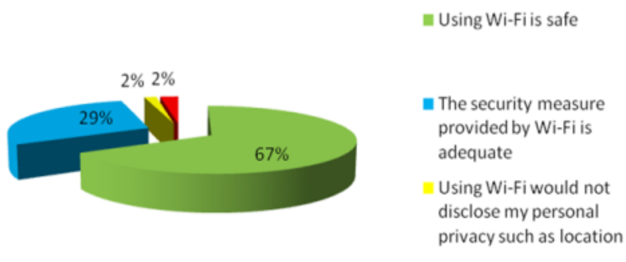
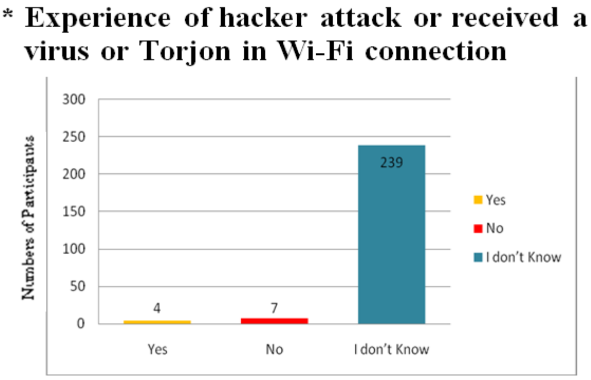
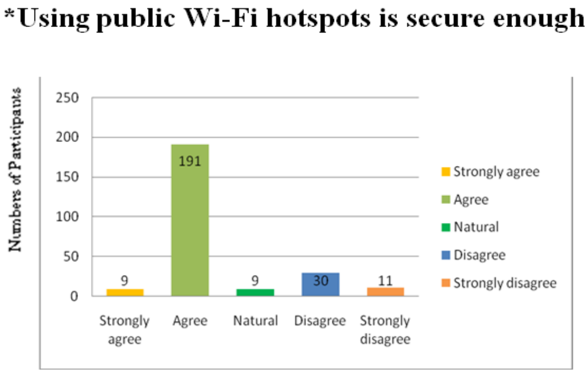


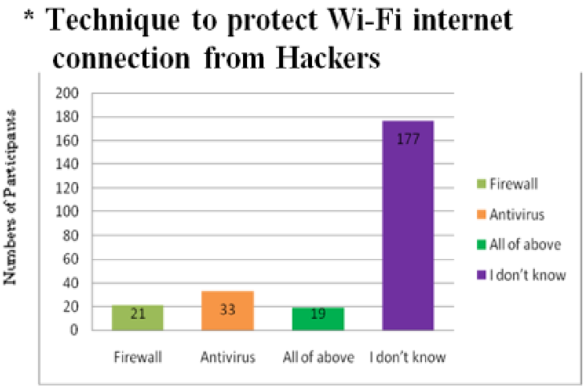
Figure.9 Perception of Wi-Fi Security



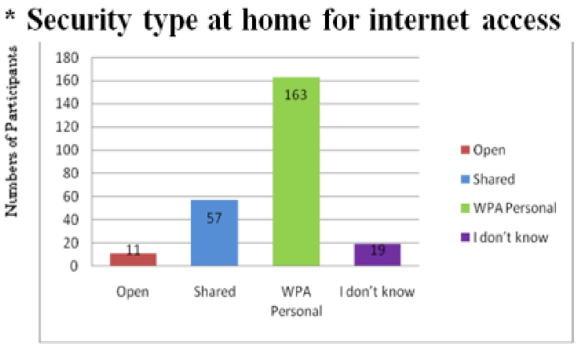
Experience of virus attack
Figure.10 Experience of virus or Torjon in Wi-Fi



Using public hotspot is safe
Figure.11 Public Wi-Fi hotspots is secure enough for internet access



Protecting technique
Figure.12 Protect Wi-Fi internet access from attackers



Wi-Fi Security techniques
Figure.13 Security techniques at home

VI. Data Analysis

6.1 The reason why participants use Wi-Fi internet connection

The study shows that respondents use it for research, doing assignment, e-learning and on-line discussion. It is also used for entertainment which include chatting, internet surfing, online shopping and e-mail checking. The Wi-Fi is used just like the internet is used. It does not matter to the user where they are and what the time is. They have little concern about time and space.

Despite the wide variety of mobile devices available in the market, the study reveals that Andriod mobile is the most prominent and dominant device used by the people in old Shahabad to access the Internet via Wi-Fi. Small, sleek, user-friendly and highly addictive due to their entertaining apps and games, Andriod phones as a leading mobile device is more popular[16]. This trend is an indicator for Wi-Fi service provider. The demand for connectivity requirement may be focused. The connectivity problems, like inadequate Wi-Fi access points, inadequate bandwidth and unstable service quality, top the list of main concerns regarding public Wi-Fi service in Old Shahabad. It can be concluded that participants are using the internet for all types of activities, including study, research work as well as for entertainment.

6.2 Wi-Fi Concern for Security – Knowledge and Wi-Fi Tethering

Security is a vital issue as participants have very poor knowledge it. The respondents are generally satisfied with Wi-Fi service in the district concerned. They don't think much of its security. Respondents were unable to identify the security implications of using Wi-Fi. They are less sure of the adequacy and safety of the Wi-Fi network. The perception of higher risk reflects the fact that some respondents are less familiar with ICT technicalities. Hence the more cautious attitude was experience while answering the question about security and safety.

The respondents' lack of confidence was evidenced by their answer regarding security questionnaires. Those who believed that they had good knowledge of Wi-Fi security, or they had the ability to explain failed to respond correctly. Their responses were the proof that they were less capable of using the security setting in Wi-Fi.

As on the issue of using Andriod phones to share Wi-Fi connection to other mobile devices known as Wi-Fi tethering. 89% respondents accepted that they used Wi-Fi tethering but 67% respondents were unable to active password protection at public places. This is the big question mark on user security knowledge. This study shows that respondents know only using Wi-Fi hotspot connection but they don't know about the threats.

The significant knowledge of the security vulnerabilities in Wi-Fi and tethering are worrisome [17]. To avoid an easy and vulnerable target for cyber attack, promotional activities should be organized to raise awareness of Wi-Fi security among the user [18]. With regard to security step must be taken to conduct training programme, so that may use Wi-Fi safely and more confidently.

6.3 Encryption and Extra Security Measures

The report shows that many home users of Wi-Fi in the district concerned are oblivious of the fact that protecting personal data through encryption alone is not enough. Steps must be taken to raise the awareness among the users of the importance of changing their Wi-Fi network SSID and administrator password [19]. Moreover, as home Wi-Fi networks are mainly used by family members, there is no point to broadcast the networks' SSID. It should be a part of education to teach users to disable their SSID broadcasts to protect their data.

6.4 Current Wi-Fi challenges that Participants Perceive

The study shows that, the users expect more power outlets and more physical places to sit or meet for longer opening times. Inadequate Wi-Fi access points, bandwidth and unstable service quality top the list of problems that frustrate Wi-Fi users. These problems occur not only with public Wi-Fi access run by commercial service providers but also with Gov. Wi-Fi hotspots. The slight difference in user evaluation of the service provided by commercial operators and that of the government is that more users agree that Gov. Wi-Fi service is better in terms of service stability, while Wi-Fi access provided by commercial operators is better in terms of bandwidth and adequacy of access points.

To turn Shahabad (Bhojpur, Buxar, Rohtas and Kaimur) into a truly wireless city requires the joint efforts of both government and the private company. Both sectors should work together to increase the number of Wi-Fi hotspots and eliminate the blind spots, i.e., locations where no Wi-Fi signal can be received, by installing, as appropriate, additional Wi-Fi hotspots or Wi-Fi signal boosters [20].

It is also important for the public Wi-Fi hotspot providers to take into account the number of simultaneous connections a hotspot can serve at a given time so that the number of public Wi-Fi users connecting to a particular Wi-Fi hotspot may not exceed the designed threshold [21]. In other words, a more systematic study needs to be conducted to estimate the number of public Wi-Fi users in each region and their Wi-Fi using pattern so that a more strategic and effective approach can be adopted when selecting Wi-Fi hotspots [22].

Lastly, inadequate transparency in service pricing has also caused concern among those who use commercial Wi-Fi hotspots. Transparency in pricing is important for fair competition and the creation of lasting customer partnerships. This report calls upon that commercial service providers showed to increase pricing transparency and urges the government to play an active role in this direction.

VII. Results and Discussions

A predominantly quantitative research approach was undertaken answer to seek the research questions. An in-depth survey was conducted in order to determine the importance and benefits of providing the Wi-Fi on Government offices, home, Public place and university campus. In addition, the task of adopting Wi-Fi at educational institutes along with different places was identified and technologies and security issues were discussed.

This study determines the issues arising when in Shahabad district of Bihar, India. Today, the need to stay seamlessly connected to the Internet, to access information on-line and to share experiences instantly and electronically has become more important than ever before. The Wi-Fi network allows us to watch YouTube and streaming releases of TV programs, to play interactive online games, to maintain constant contact with business partners, customers, families and friends whenever and wherever needed or wanted.

The research findings reveal that most of Wi-Fi user belongs to Bhojpur in comparison of three other districts (Figure.2) and a strong trend that about 65 percent of people currently use Wi-Fi at home with Personal Computer & Andriod phones as shown in Figure.7. Most of the participants approx 82% use Wi-Fi connection within last six months, it means that they are new users. 7% participants use Wi-Fi connection during last 1-2 years, their percentage is very low (Figure.3). Figure.5 shows that users are using Wi-Fi internet for entertainment. The Figure.6 presented that only 64 participants spend 3-4 hours on Wi-Fi internet and 37 respondents whole day. Approx half of the participants use Wi-Fi connection at home and approx 10% participants access Wi-Fi in University or College campus(Figure.7). 89% participants use Android phone for Wi-Fi access as shown in Figure.4. The Figure.8 explains that 91% respondents have average security knowledge about Wi-Fi and using Wi-Fi is safe as shown in Figure.9. However, many of them are lacking necessary security knowledge to prevent them from potential on-line threats and attacks. For example, more than 70% of people surveyed do not know what types of security technique are used in their Wi-Fi connection as shown in Figure.12. Among the other, who do know the type of security used? Figure.10 presents that 95% respondents have no idea about the hacker attacks (Torjon) and 76% respondents agree to access internet via Wi-Fi hotspot is secure as shown in Figure.11. Some of them cannot distinguish between security setting and encryption. At home users use mostly WPA personal security techniques(Figure.13). The lack of security knowledge in the population can be attributed to the fact that insufficient public education on Wi-Fi security was provided and the misunderstanding that setting up Wi-Fi security settings is difficult or time consuming. In addition in order to build more access points and also to encourage people to use them, government should provide more public education/training programs on Wi-Fi security and provide practical guidelines to the citizens in the future.

VIII. Conclusion

The lack of security knowledge and support would not only create on-line threats or harms to individual residents, but also block the economic growth. Among all the possible activities that can be conducted with Wi-Fi connection, the three least frequently conducted activities are financial transactions, investment and on-line purchasing. People without proper Wi-Fi security knowledge and ability to adjust such settings may feel unsafe or uncertain to conduct these activities outside their home or outside their office where they have cable internet. At the end we suggest that the government and citizens should play active roles in supporting Wi-Fi security teaching and learning by providing more resources. Because without knowledge of Wi-Fi security and their importance the use of Wi-Fi is totally unsafe.

References:

[1]. Jonathan Weiss, "Security Problems and Solutions Wireless Networks: Security Problems and Solutions", SANS Institute 2002.

[2]. AkshikaAneja, Garima Sodhi, "A Study of Security Issues Related With Wireless Fidelity (WI-FI)",International Journal of Computer Science Trends and Technology (IJCST) – Volume 4 Issue 2, Mar - Apr 2016.

[3]. Md.Alimul Haque, “On Security in Bluetooth Wireless Technology”, International Journal of Advance Research in Computer Science, Vol 2, No.5, Sept-Oct 2011.

[4]. A Rajalakshmi and G Kapilya, “The Enhancement of Wireless Fidelity (Wi-Fi) Technology Its Security And Protection Issues”, International Journal of Engineering Research and Science & Technology Vol. 3, No. 3, August 2014.

[5]. Trimintzios, Panagiotis and George Georgiou (2010), “Wi-Fi and WiMAX Secure Deployments,” Journal of Computer Systems, Networks, and Communications, 8, 2010.

[6]. Deepika Dhiman, “WLAN Security Issues and Solutions”, IOSR Journal of Computer Engineering, Volume 16, Issue 1, Ver. IV, pp 67-75, Jan. 2014.

[7]. Fong, K. K. K., & Wong, S. K. S., “Exploring the Weak Links of Internet Security: A Study of Wi-Fi Security in Hong Kong ”Network and Communication Technologies, 2(2), pp.17-28,2013.

[8]. F. Sheldon, J. Weber, S.Yoo, W. Pan, “The Insecurity of Wireless Networks.” IEEE Computer Society, vol.10, no.4, pp.54-61, July/August, 2012.

[9]. L. Wang, B. Srinivasan, N. Bhattacharjee, “Security Analysis and Improvements on WLANs”, Journal of Networks, vol. 6, no. 3, pp. 470-481, March 2011.

[10]. P. Feng, “Wireless LAN Security Issues and Solutions”, IEEE Symposium on Robotics and Applications, Kuala Lumpur, Malaysia, pp. 921-924, 3-5 June, 2012,.

[11]. M. Souppaya, K. Scarfone, “U.S Department of Commerce - Guidelines for Securing Wireless Local Area Networks (WLANs)”, Gaithersburg, MD 20899-8930: National Institute of Standards and Technology, SP 800-153, 2012.

[12]. S. Reddy, K. Rijutha, K. Ramani, S. Ali, C. Reddy, “Wireless Hacking – A Wi-Fi Hack By Cracking WEP”, IEEE 2nd International Conference on Education Technology and Computer, Shanghai, China, p. 189-193, 22-24 June.,2010.

[13]. J. Li, M. Garuba, “Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities”, Fifth International Conference on Information Technology: New Generations, Las Vegas, Nevada, pp. 557-562, 7-9 April, 2008.

[14]. D. Shiyang,”Compare of New Security Strategy With Several Others in WLAN”, IEEE 2nd International Conference on Computer Engineering and Technology, Chengdu, China, pp. 24-28, 16-18 April, 2010.

[15]. T. Stimpson, L. Liu, J., Zhang, R. Hill, W. Liu, Y. Zhan, “Assessment of Security and Vulnerability of Home Wireless Networks”, IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, pp. 2133-2137, 29-31 May, 2012.

[16]. Horrigan, John B., “Home Broadband Adoption 2008,” Pew Internet & American Life Project Survey, June 26, 2012.

[17]. Haque, Md. Alimul, Yashi Amola, and N.K. Singh, "Threat Analysis and Guidelines for Secure Wi-Fi and WiMAX Network," World Applied Programming, 2 (2), pp.110-115, 2012.

[18]. Alimul Haque, A. K. Sinha, K.M.Singh and N.K.Singh, " Security issues of Wireless Communication Networks", International Journal of Electronics Communication and Computer Engineering, Volume 5, Issue 5, 2014.

[19]. Gold, Steve , "Why WPA Standards Won't Protect Your Network," Infosecurity, 7 (1), 28–31,2010.

[20]. Md. Alimul Haque, Yashi Amola and N.K.Singh, "Performance of WiMAX over Wi-Fi with reliable QoS over wireless communication network", World Applied Programming, Vol(1), No(5), pp322-329,December 2011.

[21]. M.A.Haque, Pritam Kumar and N.K.Singh, "A review on comparative study of Wireless Networks: WiMAXVs Wi-Fi", Journal of Environmental Science, Computer Science and Engineering & Technology,Vol.2, No.3, pp 634-660,, June-August 2013.

[22]. Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends", IEEE Proceeding, arxiv:1505.07979v2, 23 April 2016.

IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) is UGC approved Journal with Sl. No. 4198, Journal no. 45125.

Alimul Haque. "Wi-Fi Adoption And Security Survey ." IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) 12.4 (2017): 67-74.