Development of Sustainable Home-Network Security Tool

Erman Hamid[1†], M. Syafiq E. Hasbullah[1†], Norharyati Harum[1†], Syarulnaziah Anawar[1†], Zakiah Ayop[1†], Nurul Azma Zakaria[1†], Wahidah Md Shah[1†],
erman@utem.edu.my
Information Security Forensics and Computer Networking (INSFORNET), Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka (UTeM)

Abstract
Home networking and its security issues are directly related. Previous studies have shown that home-network and understanding the security of it is a problem for non-technical users. The existing network management tools or ISP adapter tools are far too technical and difficult to be understood by ordinary home-network users. Its interface is not non-technical user-directed and does not address the home user's needs in securing their network. This paper presents an interactive security monitoring tool, which emphasizes support features for home-network users. The tool combines an interactive visual appearance with a persuasive approach that supports sustainability. It is not only an easy-to-use tool for all categories of home-network users but also acts as a monitoring feature for the user to secure their home-network.

Key words:
Home-network, Sustainable, Security Tools.

1. Introduction

Connecting a computer and android device to Wi-Fi is a normal activity in home-networking [1]. It's as simple as tapping on the Wi-Fi icon on the interface of computers and android phone; followed by entering the password and user will directly enter the network [2]. However, not many devices available have the ability of network management, even as simple as managing connection, up to monitoring and security handling. The fact is, security management are one of the most important element in home-network tools, since almost every home-network could experience on situations where strangers logged-in to the Wi-Fi network without permission. Although there are many features for monitoring interfaces for routers and switches in the market, even contained in Internet Service Provider (ISP) routers; the features are actually hidden and not user friendly for non-technical users [3]. It seems no such way for a non-technical user of the home-network to find out these features in Wi-Fi adapter, causing security monitoring to not be possible.

Securing the home-network become importantly critical since technology becomes more robust and vulnerable by the adaptation of various technologies such as smartphones, handhelds, tablets, and Wi-Fi router [4]. There are situations where intruders enter a Wi-Fi network and remain silent while monitoring, stalking and manipulating user data in the compromised home-network, and this is a situation that can bring great harm to users in the network. It is a result of the use of Wi-Fi in the home-network that is becoming a norm, due to its convenience in facilitating daily activities [5]. Wi-Fi offers flexibility, which means that the network can be accessed without time constraints and physical limitations; but at the same time makes it vulnerable to the entry of unknown users. It leads to the importance of a security monitoring tool (at least), which appears friendly and assisting; to help home-network users.

The problems (refer to Table 1) led to the study of the Sustainable Home-Network Security Tool (S-HoNeST), with the goal to improve the situation. The priority is to develop security monitoring tools for home-network; focusing on the android tools as the end-user platforms.

Table 1: Summary of problem statement.

No	Classification	Problem Explanation
1.	Unknown intrusion	Condition when unknown user gain access to a someone else Wi-Fi network without permission; normally by guessing the entry details (username and password), led by less secured password implemented by the Wi-Fi owner [2].
2.	Interface	Visualization of home-network interface monitoring tools that are not suitable for all groups of home-network users with less graphical and non-technical assistant features [6].
3.	Blocking	Situations where even if the owner of the Wi-Fi network knows the presence of an un-known user, features to remove (or block) the user from the network are not available in the application contained in the Internet Service Provider (ISP) adapter in the home-network. Even if it is available, remote control from mobile devices cannot be done [7].
4.	Notification	Detecting the unknown access is an important thing in ensuring that the home-network is always safe from intruders, but the ability to notify home-network owner about the intrusion is far more important [8].
5.	Awareness	Knowledge of the meaning of network security, the effects and consequences of any intrusion that occurs; is very important to be understood by owners of home-network. Without awareness, home-network owners will never take any steps in securing their network [9].

Manuscript received November 5, 2021
Manuscript revised November 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.11.35

Virtual Studio 2017 and Eclipse are further used as development tools; and S-HoNeST offers a function to scan the home wireless router (such as Tp-link router, Dlink router, Netgear router, or Huawei router, etc) the devices that are connected to the home-network. Home-network owner (user) is given a platform to manage Wi-Fi, with the ability to specify a specific user/IP address that can connect to the Wi-Fi. This function allows the Home-network owner to detects unknown users/IPs that are connected to the network, notify the home-network user, allowing to quickly identify if there is any intrusion to the network – in sustainable way.

From the research problem, this study was designed with the objective of developing a home-network security monitoring tool named Sustainable Home-Network Security Tool (S-HoNeST). Begins with defining the concept of S-HoNeST, it is followed by the design phase that focuses to the interface visualization of S-HoNeST, answering the problems described at the beginning of this study. It is aimed at giving users and home-network owners a spiritual touch called sustainability; allows users to be assisted when using the developed tools, with notifications to inform intrusions and basic network security capabilities such as blocking.

2. Related Work

The literature review conducted is related to the construction of proposed concepts, theoretical elaboration, and comparison of the existing adaptations in home-network security or monitoring tools. It was made to identify the research gaps, leading to the development of sustainable home-network security tools.

2.1 Concept

Wi-Fi is an important element in a home-network; with activity of connecting devices in the network, enabling communication by connecting all connected devices as well as connection to a Wide Area Network (WAN)[8]. The important advantages provided by Wi-Fi to the home-network user are including mobility, streaming and downloading features, and high-speed internet access with the ability to handle large files [7]. Although Wi-Fi security issues are often discussed, Wi-Fi is actually ready to come up with the ability to protect the safety of users [9].

WPA2 features with powerful security algorithms in place to protect Wi-Fi from intrusion. However, WPA2 still has weaknesses and is still able to be intercepted and could cause the home-network to be intruded. A reliable security tool with android technology adaptation is one of the solutions that can help Wi-Fi owners operate their home-network safely [6]. It comes in the form of a sustainable security application that drives form the helpful interface visualization, allowing users to operate the home-network in optimum performance - easily and safely, from their hand-held devices such as smartphones or tablets (refer to Fig. 1) [10].

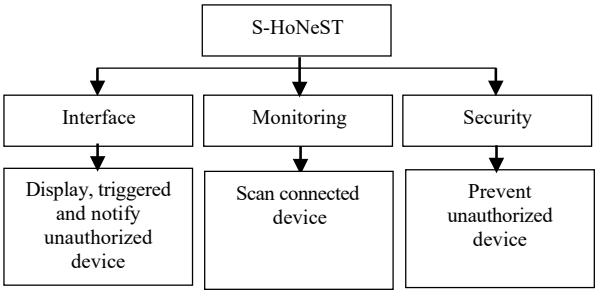

Fig. 1 Concept.

2.2 Theory

Wi-Fi The basic principle of a security tool for home-network is the ability to prevent any intrusion from unauthorized or suspicious enter into the network [11]. The device must able to scan all entries into the network with the ability to display Internet Protocol (IP) address or Medium Access Control (MAC) address (or both) - using Address Resolution Protocol (ARP)[12]. Theoretically, when unauthorized devices are detected entering the network, it is known to the home-network owner through notifications and the option is to let the devices remain in the network or block. ARP that binds data from layer 2 and layer 3 of the Open System Interconnection (OSI) model is required for the process of translating IP addresses to MAC addresses [13].

All Layer 2 OSI Model hardware (including switches, routers, and access points) has an ARP table that stores physical address information (MAC address) and logical address (IP address) [14]. ARP is used for communication between hosts in the network, with the address on the Network Interface Card (NIC) being the identity of each connected host. ARP is a request-reply -*protocol that requests the MAC address and the neighbour device; that sends ARP to reply messages to send the requested MAC address [12]. This is the basis of the connection created between two established hosts, which allows the security monitoring tool to know the entry of each device into the network. Fig. 2 shows the proposed ARP flow of S-HoNeST, showing the interaction between the home-network tool and its environment.

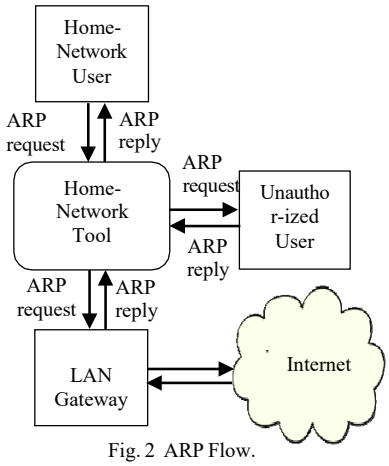

Fig. 2 ARP Flow.

2.3 Application

Comparative reading was performed on twenty-one Wi-Fi security tools available in the market or used in studies related to network security, with the classification of the interface type – either Graphical User Interface (GUI) or not; and the use of each tool – the type of Operating System (OS). The applications are Advanced IP Scanner [15], Acrylic Wi-Fi [16], Angry IP Scanner [17][18][19], Fing [20], Insider [21], Kismet[22], Meraki Wi-Fi Stumbler [20], Netcut [23][24], Netspot [25], Network Scanner [20], Paessler PRTG [26], Personal Network Packet Sniffer [20], ScanFi [20], Tuxcut [27][28], Who is on my Wi-Fi [29], Wi-Fi Analyzer [30], Wi-Fi Scanner [20], Wi-Fi Thief Detector [31], Wireless Network Watcher [20][32][33], Wireshark [34][35], and Vistumbler [36].

Most of them are GUI type tools, but not home-network android based tools. From the readings conducted, five tools are shortlisted due to the elements used that fit the problems and objectives outlined in the S-HoNeST development study. The comparative review of the five selected tools is shown in Table 2; and details comparison are made to the selected features including parameters of packet capturing, block method of ARP, spoofing technique, notification ability, and interface visualization method that can catalyse sustainability.

A good network assistance/management/monitoring tool must have the visualization interface that helps users explore the functions available on the tool. Regardless of the technical level of the user and the type of tool; the interface should completely reduce the differences between the user and the system, allowing the user to interact with the tool well. Good visualization features including easy to remember, efficient, and easy to learn; allows users to understand and be able to use the tool easily and sustainably.

Table 2: Comparative Study.

	Netcut	**Tuxcut**	**Advanced IP Scanner**	**Wireless Network Watcher**	**Wireshark**	**Proposed Solution**
Author	[29][21]	[30][31]	[32][33]	[34][35]	[27][36]	**S-HoNeST**
Packet Capture Library	Win-Pcap	libcap	Win-Pcap	Win-Pcap	pcap	**Win-Pcap**
Block Method	Yes	Yes	Yes	-	-	**Yes**
Visualization Interface	Not User Friendly	User Friendly	User Friendly	User Friendly	Not User Friendly	**User Friendly**
Blocking Technique	ARP Spoofing	ARP Spoofing	ARP Spoofing	No	No	**ARP Spoofing**
Notification	-	-	-	Yes	-	**Yes**
User	Experience user	Expert user	Experience user	Experience user	Expert user	**All type of user**

3. Method and Proposed Solution

3.1 Methodology

Prototype Model is chosen to ensure coding can be continued on the same time requirements are obtained [16]. Prototype model is a software development model that is used to help prototypes that are built to understand requirements [37]. Prototypes are developed based on known requirement needs; which allows the user to better understand the needs of the desired system [38]. There stages included project planning, problem analysis, system design, implementation, testing, and maintenance. Every stage is important and the flow of the process can be referred to Fig. 3.

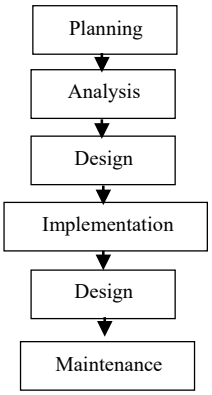

Fig. 3 Prototyping methodology.

3.3 Proposed Solution

Moving forward from the research problems, S-HoNeST finally proposed as the solution. S-HoNeST was developed in the form of a home-network security

monitoring tool; equipped with the ability to scan the Wi-Fi to detect unauthorized device in the network. S-HoNeST has the ability to notify Wi-Fi owners where it uses WinPcap Library to capture traffic and ARP spoofing technique for the process of disconnecting from the host to the network. The unauthorized device information will be sent in the form of notifications and displays to be interpreted by the home-network owner. S-HoNeST interactions with users are developed with easy-to-understand interface variables and catalyze sustainability. Visual C# language is used in this project as a script of the software because of the ability to allows a complex program to be broken into simpler programs called functions (refer to Fig. 4).

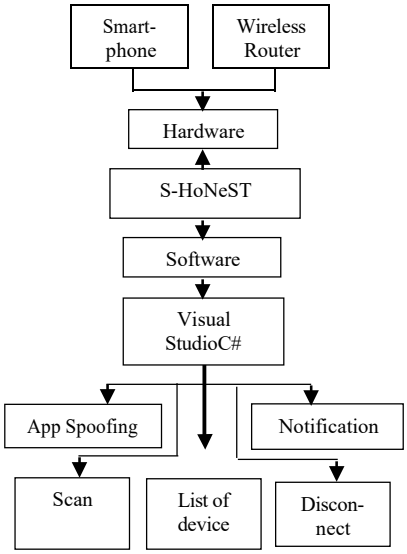

Fig. 4 Proposed solution.

4. Implementation

This section describes the hardware implementation and functionality of the Home-Network Security Tool. The Wi-Fi router, as the gateway to the network, will be pre-configured with a security password to ensure the network is up and able to connect the home-network to the WAN with security controls. S- HoNeST forming an integration between the monitoring tools and the Wi-Fi router; as a platform for network protocol to send all of the captured MAC address to home- network monitoring tool. Overall, S-HoNeST is divided into hardware connection and application functionality.

4.1 Hardware Connection

Fig. 5 shows the possible connection of hardware in home-network which includes Wi-Fi router and other devices that connected in the network. It might include hardware such as computers, laptops, smartphones and tablets that used to access the Wi-Fi router in getting the networking or internet connection. All of the device must ready with Home Wi-Fi Security Tool installed in it which caused it ability to scan the home-network to monitor the connected devices. The notification to the Wi-Fi owner will be triggered if any unauthorized device access the network.

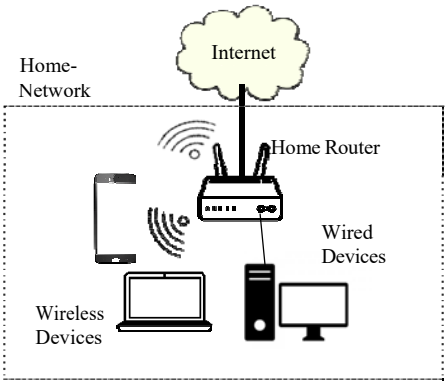

Fig. 5 Hardware connection.

4.2 Application Functionality

S-HoNeST is a network security monitoring tool, that uses C# language, Visual C# platform, and WinPcap library software to ensure suspicious entries can be scanned and detected. Fig. 6 shows the functionality of the Home Wi-Fi S-HoNeST in details including the task force of the tools including list of MAC address, list of devices, list of IP address, scanning and notification.

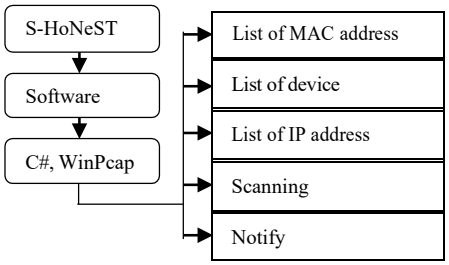

Fig. 6 Functionality of Home-Wife Security Tool.

4.3 Application Flow

Fig. 7 shows the flow of S-HoNeST. It starts with the home-router displaying the interface asking for an access password. When the connection is confirmed, the home-network owner is given the right to monitor and scan the Wi-Fi network. Next, the detection of unauthorized users who are in the network is displayed in the form of a table, which is displayed in the interface of the android application after the notification given by the home-router to the Wi-Fi owner. The Wi-Fi owner will decide whether to block the user or leave it in the network.

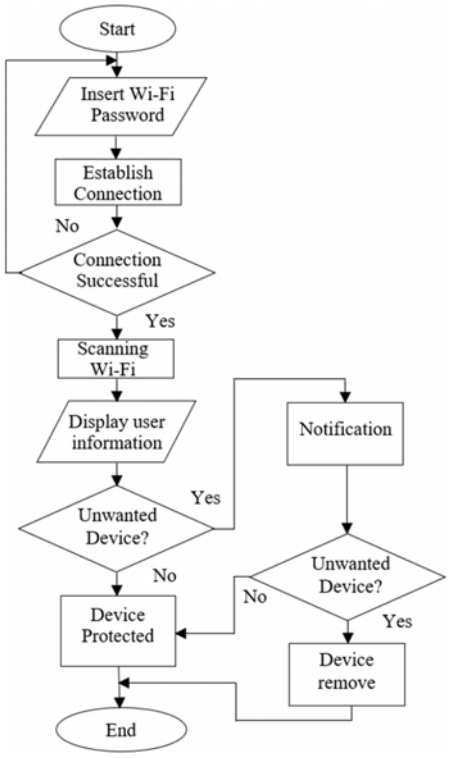

Fig. 7 The flow of S-Honest.

4.4 Interface Design

The interface of the S-HoNeST introduce the sustainability features as an essential element to the visual that connect user to the application. It is featured with memorizing, understanding, explaining, and picturing abilities as the visualization features; along with the adaptation of sustainability features including persuading, influencing, guiding and driving ability [39][40]. The coordination of these two interface techniques is combined in performing basic behaviour of S-HoNeST including sending notifications, listing the connected devices, and viewing the scanned network element.

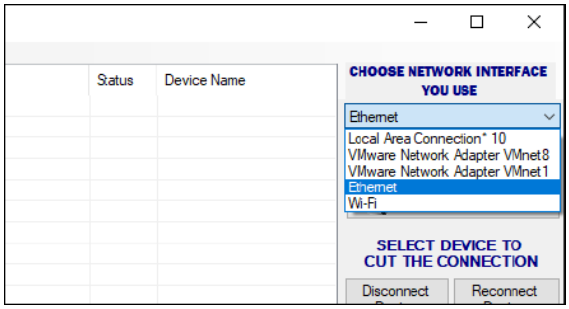

Fig. 8 Main interface design.

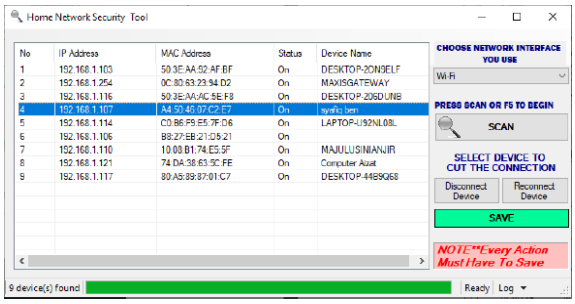

Fig. 9 Scanning interface, listing and renaming devices.

4.5 Analysis and Result

The S-HoNeST prototype is then developed and evaluation of this prototype is carried out using three testing methods shown in Table 3.

Table 3: Summary of testing activity.

Hardware Testing	• Hardware testing including Wi-Fi Router, personal computer and android smart phones. • Wi-Fi router is prepared to be accessed, while personal computers and android smartphones are ensured to be in good condition. • Wi-Fi connection is tested by disconnect and reconnect the Wi-Fi to ensure the router is working properly.
Application Testing	• Every created function of the S-HoNeST are tested and run correctly. *Unit Testing* • Check the source code to ensure no error and working properly. *Home-network Security Tool* • Manually test the application
Acceptance Testing	• Acceptance testing was conducted on 10 random home-network users. • Respondents were given 10 minutes' times using the S-HoNeST prototype, and a brief interview session was conducted to identify consumer acceptance. • The conclusions obtained from this questionnaire indicate that majority of the respondents satisfy with the S-HoNeST prototype.

5. Discussion

Home-Network Security Tool (S-HoNeST) is an intermediate level Wi-Fi security software. S-HoNeST is an android application that created by the C# language to perform all functionality of the software such as scanning the network, retrieve device information, notify, disconnect device and reconnect device. Specifically, S-HoNeST is developed for the home use and help family member who are not know how to monitor their Wi-Fi using another software or router firmware. It will ease the home-network owner to prevent the network from unauthorized user.

The S-HoNeST testing phase showed that the prototype worked well, covering hardware and software elements; up to acceptance testing that targets brief interviews related to the functionality, interface, and satisfaction to S-HoNest. The brief interview sessions focused on three basic questions; (i) satisfaction regarding the functionality of the tool, (ii) the level of acceptance of the interface, (iii) the influence of S-HoNeST to the usability.

*Question(i): Is the S-HoNeST **functionality** sufficient for your needs of monitoring your home-network (Yes/NotSure/No)? Why?*

65% of respondents agreed that the functionality available on S-HoNeST is sufficient, 25% are not sure, while another 10% think it can still be improved. There are suggestions that the functionality of S-HoNest be added with more extensive network management functions such as packet spoofing, virus scanning and dual-interface mode to be adjusted between graphical and command line needs.

*Question(ii): Is the S-HoNeST **interface** visualization friendly to you (Yes/NotSure/No)? Why?*

85% of respondents agreed that the S-HoNeST interface is user friendly, 10% are not sure, while another 5% think it can still be improved. They feel that the interface display is direct and easy to use, not too informative and clear. There are suggestions to use more graphics in the form of icons, by reducing the use of picons to add ease of user usability.

*Question(iii): After using S-HoNeST, do you feel that your home-network is **secured** (Yes/NotSure/No)? Your opinion?*

83% of respondents agreed that S- HoNeST, 6% are not sure, while another 11% think it can still be improved. S-HoNeST makes them comfortable with the security status of their network especially in terms of knowing whether their network is intruded or not. They agreed that the management of such tools should be available to every home-network owner.

6. Conclusion

In accordance with the term of h-o-n-e-s-t on S-HoNeST, this security monitoring tool does appear to sincerely notify and list all devices that have entered the network. This research has explored the challenges of proposing security monitoring tools for home-network. It is equipped with monitoring and security solutions that allow home-network users to feel safer from intruder's interference on their respective networks. It includes visualization and persuasive coordination, which forms a tool aimed to support sustainable use for home-network user. Briefly, the advantages of S-HoNeST are as follows:

a) *Sustainable-friendly interface visualization to manage home Wi-Fi*

S-HoNeST consists of a sustainable-friendly interface that focuses on the visualization of the design and the user's ability to use the tool independently. The interface visualization is important by the objective to allow users to interact well with the tools being used, with coordination of sustainability-friendly features such as direct and easy to understand, memorability, efficiency, and learnability.

b) *Real time scan and alert for notification*

S-HoNeST provides a real-time notification alert which beep sound and dialog message to the Wi-Fi owner if there are any unauthorized access detected. Wi-Fi owner can take an immediate action to the unauthorized access, to permit or to deny.

c) *Naming function for device name*

Wi-Fi owner can decide to save the name (default name is unknown device) or give a new name for every device that listed in a list. S-HoNeST will send a beep to the android application of home-network user for every device that has no device name. It will help the Wi-Fi owner to identify that there are un-registered user that might be unauthorized access to the network.

Acknowledgments

The authors would like to thank the INSFORNET, Fakulti Teknologi Maklumat dan Komunikasi (FTMK), Universiti Teknikal Malaysia Melaka.

References

[1] R. Yu, X. Zhang, and M. Zhang, "Smart Home Security Analysis System Based on the Internet of Things," in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2021*, 2021, pp. 596–599, doi: 10.1109/ICBAIE52039.2021.9389849.

[2] N. Castelli, C. Ogonowski, T. Jakobi, M. Stein, G. Stevens, and V. Wulf, "What Happened in my Home ?: An End-User Development Approach for Smart Home Data Visualization," in *2017 CHI Conference on Human Factors in Computing Systems*, 2017, pp. 853–866.

[3] E. Hamid, M. C. Ang, and A. Jaafar, "A Comparative Study on Visualization Technique for Home Network," in *Progress in Intelligent Decision Science*, 2021, pp. 71–85.

[4] V. C. Shekar, S. U. Rahman, S. V. B. DB, A. Mateen, and R. A.S, "Enhanced Network Security for IoT based Home Automation System," *Int. J. Emerg. Res. Manag. Technol.*, vol. 6, no. 6, p. 278, 2018, doi: 10.23956/ijermt.v6i6.282.

[5] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A Survey of Securing Networks Using Software Defined Networking," *IEEE Trans. Reliab.*, vol. 64, no. 3, pp. 1086–1097, 2015, doi: 10.1109/TR.2015.2421391.

[6] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," in *2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016*, 2016, pp. 364–367, doi: 10.1109/ICBDSC.2016.7460395.

[7] A. Crabtree, R. Mortier, T. Rodden, and P. Tolmie, "Unremarkable networking: the home network as a part of everyday life," *Proc. Des. Interact. Syst. Conf. ACM.*, pp. 554–563, 2012, Accessed: Mar. 20, 2014. [Online]. Available: http://dl.acm.org/citation.cfm?id=2318039.

[8] A. Moallem, "Why should home networking be complicated?," in *Advances in Usability Evaluation: Part II, CRC Press*, 2013, pp. 4169–4178.

[9] R. Mortier *et al.*, "Control and understanding: Owning your home network," *2012 Fourth Int. Conf. Commun. Syst. Networks (COMSNETS 2012)*, pp. 1–10, Jan. 2012, doi: 10.1109/COMSNETS.2012.6151322.

[10] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Benefits and risks of smart home technologies," *Energy Policy*, vol. 103, no. January, pp. 72–83, 2017, doi: 10.1016/j.enpol.2016.12.047.

[11] G. Conti and K. Abdullah, "Passive visual fingerprinting of network attack tools," in *VizSEC/DMSEC '04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, 2004, pp. 45–54, doi: 10.1145/1029208.1029216.

[12] J. L. Chen and K. C. Yen, "Transparent bridging support for bluetooth-IP service interworking," *Int. J. Netw. Manag.*, vol. 12, no. 6, pp. 379–386, 2002, doi: 10.1002/nem.454.

[13] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, and P. Burnap, "EclipseIoT: A secure and adaptive hub for the Internet of Things," *Comput. Secur.*, vol. 78, pp. 477–490, 2018, doi: 10.1016/j.cose.2018.07.016.

[14] W. Rahman, P. T. Nguyen, M. Rusliyadi, E. Laxmi Lydia, and K. Shankar, "Network monitoring tools and techniques uses in the network traffic management system," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 11, pp. 4182–4188, 2019, doi: 10.35940/ijrte.B1603.0982S1119.

[15] A. Rahman, K. R. Kawshik, A. A. Sourav, and A.-A. Gaji, "Advanced Network Scanning," *Am. J. Eng. Res.*, no. 5, pp. 38–42, 2016, [Online]. Available: www.ajer.org.

[16] W. Da Chen and Z. X. Lin, "A Prototype Development of the Smart Mousetrap System Equipped with LoRa," 2018, doi: 10.1109/ICCE-China.2018.8448569.

[17] S. Ibnu Hunais, M. Yamin, "Penerapan Keamanan Jaringan Menggunakan Metode Host Based IDPS WLAN dan LAM Berbasis Web dan SMS Gateway," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, p. 97, 2020.

[18] M. A. Doshi and P. Sharma, "Digital Forensics Analysis for Network Related Data," *Int. Res. J. Eng. Technol.*, vol. 7, no. 4, pp. 1390–1398, 2020.

[19] D. Avasthi, "Network Forensic Analysis with Efficient Preservation for SYN Attack.," *Int. J. Comput. Appl.*, vol. 46, no. 24, pp. 17–22, 2012, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Network+Forensic+Analysis+with+Efficient+Preservation+for+SYN+Attack#0.

[20] C. Science, S. Madden, T. Supervisor, and A. Smith, "iNav: A Hybrid Approach to WiFi Localization and," 2008.

[21] M. R. Kurniawan and L. O. Sari, "Analisis Sistem Keamanan Wireless Local Area Network (Wlan) Pada Proses Tethering," *Jom FTEKNIK*, vol. 5, no. 2, pp. 1–7, 2018.

[22] E. Nasr, M. Jalloul, J. Bachalaany, and R. Maalouly, "Wi-Fi Network Vulnerability Analysis and Risk Assessment in Lebanon," *MATEC Web Conf.*, vol. 281, p. 05002, 2019, doi: 10.1051/matecconf/201928105002.

[23] M. Akbar, "Perancangan Software Ids Snort Untuk Pendeteksian Serangan Interruption (Netcut) Pada Jaringan Wireless," *J. INSTEK (Informatika Sains dan Teknol.*, vol. 3, no. 1, pp. 121–129, 2018, doi: 10.24252/instek.v3i1.5007.

[24] J. A. Yani, N. Palembang, and S. Selatan, "Evaluasi Penerapan Autentikasi Pengguna Wireless LAN Berbasis Radius Server Universitas Bina Darma," *J. Mhs. Tek. Inform.*, no. 12, 2014.

[25] M. Mongiovì, P. Bogdanov, R. Ranca, E. E. Papalexakisy, C. Faloutsos, and A. K. Singh, "NetSpot: Spotting significant anomalous regions on dynamic networks," in *Proceedings of the 2013 SIAM International Conference on Data Mining, SDM 2013*, 2013, pp. 28–36, doi:

10.1137/1.9781611972832.4.
[26] Z. Ali, F. Naz, Javed, M. Qurban, M. Yasir, and S. Jehangir, "Analysis of VoIP over wired & wireless network with implementation of QoS CBWFQ & 802.11e," *Int. J. Comput. Netw. Inf. Secur.*, vol. 12, no. 1, pp. 43–39, 2020, doi: 10.5815/ijcnis.2020.01.05.
[27] N. A. Fadzil and N. Jaafar, "Sikap Pelajar Sekolah Menengah Arab Jabatan Agama Islam Melaka Terhadap Pembelajaran Bahasa Arab," *e-Prosiding PASAK 4. 24-25 April 2019*, vol. 4, no. April, pp. 191–202, 2019.
[28] A. Almaarif and S. Yazid, "ARP Cache Poisoning sebagai Teknik Alternatif untuk Membatasi Penggunaan Bandwidth berbasis Waktu," *J. Rekayasa Sist. Ind.*, vol. 5, pp. 108–113, 2018, doi: 10.25124/jrsi.v6i1.367.
[29] J. Hong, A. Levy, L. Riliskis, and P. Levis, "Don't talk unless i say so! securing the internet of things with default-off networking," in *Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI 2018*, 2018, pp. 117–128, doi: 10.1109/IoTDI.2018.00021.
[30] T. Al-Kadi, Z. Al-Tuwaijri, and A. Al-Omran, "Arduino Wi-Fi network analyzer," in *Procedia Computer Science*, 2013, vol. 21, pp. 522–529, doi: 10.1016/j.procs.2013.09.073.
[31] A. Setiawan and A. I. Purnamasari, "Pengembangan Smart Home Dengan Microcontrollers ESP32 Dan MC-38 Door Magnetic Switch Sensor Berbasis Internet of Things (IoT) Untuk Meningkatkan Deteksi Dini Keamanan Perumahan," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 3, pp. 451–457, 2019, doi: 10.29207/resti.v3i3.1238.
[32] R. C. Joshi and E. S. Pilli, "Network Forensic Tools," in *Fundamentals of Network Forensics.*, 2016, pp. 71–93.
[33] D. Gajjar and A. Prajapati, "EasyChair Preprint Working of Offline Cloud Storage Using FTP , RDP and RPC with Router," *Am. J. Eng. Res.*, vol. 5, no. 6, pp. 38–42, 2020.
[34] V. Ndatinya, Z. Xiao, V. R. Manepalli, K. Meng, and Y. Xiao, "Network forensics analysis using Wireshark," *Int. J. Secur. Networks*, vol. 10, no. 2, pp. 91–106, 2015, doi: 10.1504/IJSN.2015.070421.
[35] I. P. A. E. Pratama and P. A. Dharmesta, "Implementasi Wireshark Dalam Melakukan Pemantauan Protocol Jaringan (Studi Kasus : Intranet Jurusan Teknologi Informasi Universitas Udayana)," *Mantik Penusa*, vol. 3, no. 1, pp. 94–99, 2019.
[36] D. E. Goncharov, S. V. Zareshin, R. V. Bulychev, and D. S. Silnov, "Vulnerability analysis of the Wifi spots using WPS by modified scanner vistumbler," in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2018*, 2018, vol. 2018-Janua, pp. 48–51, doi: 10.1109/EIConRus.2018.8317027.
[37] S. A. Soomro, H. Casakin, and G. V. Georgiev, "Sustainable design and prototyping using digital fabrication tools for education," *Sustain.*, vol. 13, no. 3, pp. 1–17, 2021, doi: 10.3390/su13031196.
[38] B. Camburn *et al.*, "Design prototyping methods: State of the art in strategies, techniques, and guidelines," *Des. Sci.*, vol. 3, 2017, doi: 10.1017/dsj.2017.10.
[39] E. Hamid, N. Bahaman, A. Jaafar, A. M. Choo, and A. A. Malek, "Development of home network sustainable interface tools," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 72–76, 2019, doi: 10.14569/ijacsa.2019.0100210.
[40] N. binti Harum, N. A. Zakaria, N. A. Emran, Z. Ayop, and S. Anawar, "Smart book reader for visual impairment person using IoT device," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 251–255, 2019, doi: 10.14569/ijacsa.2019.0100233.

Erman Hamid is a Senior Lecturer at faculty of ICT, Universiti Teknikal Malaysia (UTeM). He received BIT (Hons) from Universiti Utara Malaysia and MIT (Computer Science) from Universiti Kebangsaan Malaysia. His research area are Internet of Things (IoT) and Network Visualization.

M. Syafiq E. Hasbullah is an IT Executive at Top Glove. He received Bachelor in Computer Science (Computer Networking) from Universiti Teknikal Malaysia Melaka (UTeM). His research area is Network Security Tool.

Norharyati Harum holds her bachelor's in engineering (2003), MSc. in Engineering (2005) and PhD in Engineering (2012) from Keio University, Japan. She is currently a senior lecturer at Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM). Her interests in research area are Internet of Things (IoT), Smart Applications, Embedded System, Wireless Sensor Network, Next Generation Mobile Communication, Radio Frequency Planning and Signal Processing. She is an accomplished inventor, holding patents to radio access technology, copyrights of products using IoT devices.

Syarulnaziah Anawar holds her Bachelor of Information Technology (UUM), Msc in Computer Science (UPM), and PhD in Computer Science (UiTM). She is currently a Senior Lecturer at the Faculty of Information and Communication Technology, UTeM. She is a member of the Information

Security, Digital Forensic, and Computer Networking (INSFORNET) research group. Her research interests include human-centered computing, participatory sensing, mobile health, usable security and privacy, and societal impact of IoT.

Zakiah Ayop holds BSc. in Computer Science (2000) from UTM and MSc in Computer Science (2006) at UPM. Currently she is a senior lecturer in Faculty of Information and Communication Technology (FTMK), Universiti Teknikal Malaysia Melaka (UTeM). She is a member of the Information Security, Digital Forensic, and Computer Networking research group. Her research interest are Information System, Internet of Things (IoT) and Network and Security.

Nurul Azma Zakaria graduated with B.Eng in Electronic Computer Systems and MSc in Information System Engineering from Salford University and UMIST, UK respectively. She received her PhD in Information and Mathematical Sciences from Saitama University, Japan. As senior lecturer in Universiti Teknikal Malaysia Melaka (UTeM), she explores various research themes related to engineering and ICT, specifically in System-Level Design, Embedded System, Internet of Things (IoT), IPv6 Migration and 6LoWPAN.

Wahidah Md Shah is a Senior Lecturer in Department of Computer System and Communication, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia. Her research spans System and Networking, Network Security and IoT related technology.