ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

IMPROVING IOT SECURITY: EXPLORING BLUETOOTH, WI-FI, AND HUB VULNERABILITIES IN SMART HOMES

Mohd Saud[1], Chirag Maheshwari[2], Shafiqul Abidin[3]
[1]Department of computer science Aligarh Muslim University Aligarh-202002, Uttar Pradesh, India saudmohd862@gmail.com
[2]Department of Computer Science, Aligarh Muslim University, Aligarh-202002, Uttar Pradesh, India chirag.maheshwari135408@gmail.com
[3]Department of computer science Aligarh Muslim University Aligarh-202002, Uttar Pradesh, India shafiqulabidin@yahoo.co.in

ABSTACT:
The study looks into the security landscape of the smart home IoT ecosystem based on the involvement of Bluetooth and Wi-Fi in it, and with smart hubs. These communication protocols and central controllers are widely being used in homes, where their vulnerabilities create a high degree of risk. This approach is proposed scientifically, as it comprehensively identifies and analyzes the existing security risks, encryption strategies, authentication mechanisms, and overall security robustness in smart home devices. Our results emphasize the dire need for an integrated security approach that would safeguard an emerging industry on home IoT hardware. Building on previous work in IoT vulnerabilities, this study strongly supports the multiple vectors involved in securing the consumer environment. Applying intelligent security practices to every fresh installation a potential user can make enables them to contribute to making the home ecosystem safer and smarter.
Keywords: Wi-Fi, Bluetooth, Internet of Things (IoT), IoT Vulnerabilities, Smart Hubs, ZigBee, PENTOS

1. Introduction

The integration of new devices into the home network characterizes exponential growth in the IoT. The same connectivity, while reaping great benefits through better monitoring, automation, and smooth communication, also presents tremendous challenges in terms of security. With more IoT devices becoming common, they introduce new attack vectors, hence making such networks vulnerable to cyber threats. Most IoT smart home devices, especially the ones working on wireless communication protocols such as Bluetooth or Wi-Fi, usually lag behind when it comes to proper cyber security implementations. More significantly, smart hubs are an essential part of any IoT environment; they also include a number of smart devices, which makes them yet another weak point. The intent of this journal is a preliminary analysis of the security threats of Bluetooth, Wi-Fi, and smart hubs in home IoT ecosystems. With more IoT devices being used within the home, the area of vulnerabilities for these key components is becoming significantly relevant. common user of these devices is concerned because of the internet of things' vulnerability to cyber attacks because of their unique characteristics and weak configurations [1].

2. LiteratureReview

The ever-increasing dependence of IoT devices on Bluetooth and Wi-Fi as main communication technologies has brought seamless connectivity to smart homes. This convenience, however,

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

comes with serious security dangers: the proliferation of linked devices brought about by the advancement of these technologies raises many questions regarding encryption, authentication, and general security. Past research has identified crucial vulnerabilities: improper authentication procedures, susceptible to eavesdropping, and unauthorized access. The timeline relating to security vulnerabilities of IoT devices underlines the gravity with which these insecurities need to be addressed. Device hijacking, data breach incidents, and the transmission of information over unsecured channels pose serious threats. The aim of this work is to systematically investigate the security implications of Bluetooth- and Wi-Fi-enabled IoT devices in homes and buildings.Wireless sensor networks and IoT are major areas in computer science. Wireless sensor networks and IoT hold great economic and industrial significance [2].

3. Types of Security Attacks Present in Widely Used IoT Environments

Table1: Various types of attacks targeting IoT devices, classified based on their methods, protocols, and detailed descriptions.

AttackType	Protocol	Description
RogueDevice Connections	Wi-Fi	AttackerssetuprogueWi-FiaccesspointstotrickIoTdevicesintoconnectingtothem, exposingthemtorisks.
	Bluetooth	Attackersimpersonate legitimate Bluetoothdevicesto establish unauthorized connections.
Firmware Exploitation	Wi-Fi	Vulnerabilitiesin firmwaremaybeexploitedtogaincontroloverthedeviceor install malicioussoftware.
	Bluetooth	SimilartoWi-Fi,vulnerabilitiesinfirmwarecanbeexploitedtomanipulatedevicefunctionsor install malware.
Zero-DayExploits	Wi-Fi	Attackstargetingunknownvulnerabilitiesinprotocolsorsoftwarecanposeasignificantthreat until patched
	Bluetooth	Zero-dayexploitsinBluetoothprotocolsorsoftwarecanalsoposesignificant threatsuntilpatches are released
Eavesdropping	Wi-Fi	Unsecuredchannelscanbeexploitedtoeavesdroponsensitiveinformationtransmitted betweendevices and networks
	Bluetooth	SimilartoWi-Fi,unsecuredchannelsinBluetoothcanbeexploitedforeavesdropping on sensitive information
Man-in-the-MiddleAttacks	Wi-Fi	AttackersinterceptandaltercommunicationbetweentheIoTdeviceandnetwork,leadingtounauthorizedaccess..
	Bluetooth	AttackersinterceptBluetoothcommunication,allowingforeavesdroppingorinjectionofmalicious data.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Denial-of-Service Attacks	Wi-Fi	OverloadingWi-FinetworkswithexcessiverequestscandisruptserviceforIoTdevices.
	Bluetooth	JammingBluetoothfrequenciescandisruptdevicecommunication,renderingthemunabletocommunicateeffectively.
Blue jacking andBluesnarfing	Bluetooth	Bluejackinginvolvessendingunsolicitedmessages,whilebluesnarfingtargetsunauthorizedaccess todevice data.
Credential Attacks	Wi-Fi	Brute-forceattacksorcredentialinterceptioncancompromisedevicesecurity,allowingunauthorizedaccess.
	Bluetooth	SimilartoWi-Fi,credentialattackscancompromiseBluetoothdevicesecurity,leading to unauthorizedaccess.

This table is used to categorize hacking techniques targeting different varieties of IoT devices by the respective attacks, protocols, and descriptions. It can also be an important reference in identifying the range of threats that prevail as security threats in IoT, especially those related to the Wi-Fi-and Bluetooth-enabled devices.The denial-of-service attacks are considered one of the major threats that are faced by IoT devices in smart homes. In a DoS attack, all devices connected through a Wi-Fi network will be disconnected and nobody is allowed to reconnect[3]. This can cause damaging and inconvenient impacts on smart home systems and users make them more vulnerable to system malfunction and potential security breaches.

Additionally, most users select the easy way of accessing an account over security purpose by using weak patterns other than the strong one. easy-guess passwords facilitate brute force attacks in which an attacker will attempt all combinations of user-name and password until a proper match is found on both ends [4]. This happens on both types of IoT devices, with or without Wi-Fi and Bluetooth operation.

Table 2*:* **Digital risks associated with various smart home devices**.

	Privacy Intrusion	Hacking	Malware	DoS	Stalking
Security and Surveillance	10	.9	.7	12	2
Lighting control ,smart bulb	7	12	.9	.9	1
Voice control device.	7	10	4	5	1
Temperature and Ventilation	4	6	6	5	3
Smart home app or browser	.4	7	.6	3	1

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Occupancy-aware control.	4	6	6	5	1
Smart plug	5	.8	5	4	1
Automation elderly/sick	7	2	1	1	1
Entertainment	2	3	5	5	2
WiFi	2	4	1	5	0
Smart Kitchen	0	4	3	1	0
Smart grid and Smart meter	3	0	0	0	0
Leak detector and air quality	1	2	2	2	1
Pet or baby care	1	1	1	2	0
Cleaning robot	1	1	0	1	0

Additionally, this table also provided the forms of data involved in the digital risk in varied situations, and the harms discovered for some of the smart home devices indicated in Table 2, within which their results showed the fact that security/surveillance devices are more likely to be hacked, followed by the Wi-Fi connected, while cleaning robots seem to be at a lower risk [5]. As all these devices rely on Wi-Fi or Bluetooth for transmitting data, consumers should undertake their own research, very diligently and with great caution, about the brands and products currently available, especially their record in terms of breaches involving these communication technologies.

Another researcher scanned 22 smart gadgets and found 17 vulnerabilities that have been later published as new CVEs [6]. Each of the weaknesses presents a significant risk to the functionality and security of smart home systems and can potentially enable attackers to compromise IoT services. These gadgets are sold worldwide for personal use, and due to this, these vulnerabilities need to be addressed to ensure that users of smart home gadgets maintain their privacy and safety.

Vulnerabilities Across Different Wireless Protocol Versions

Table 3: Types of Attacks, Targeted Wireless Protocols, Vulnerability Descriptions, and Exploitation Techniques

AttackType	Protocol	Description	Tools/MethodsUsed
AttackingWEP	Wi-Fi	WEPisvulnerabletobrute-forceattacksandcanbecompromisedwithin minutes usingtoolslikeAircrack..	Aircrack
AttackingWPA2	Wi-Fi	WPA2canbetargetedthroughbruteforcingWPSPIN,similartoWPAattacks,withtoolslikeReaver.	Reaver

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Several experiments by a researcher show significant susceptibilities of Wi-Fi protocols that should also motivate IoT manufacturers to act in a timely manner. WEP and WPA2 are found to be easily cracked with the help of Aircrack or Reaver, raising a serious question about potential breaches in security that may concern user privacy and data integrity [7].Wireless sensor networks are prone to security threats such as authenticity, confidentiality, and data integrity. Sensor nodes are susceptible to DOS and flood attacks, which lead to data loss. Security is needed to avoid network attacks [8].

Another general wireless communication technology for IoT devices with low power, short range is ZigBee. Some of the threats in this technology exist.Reconnaissance, where attackers collect information to use later, DoS, where the functionality of a system is affected, hijacking, where unauthorized parties take over legitimate devices, and malicious control, where attackers assume a form of existing trusted devices to gain unauthorized access are some of the other potential attacks against ZigBee [9].
Similar issues are reflected in home IoT gardens from agriculture. LoRaWAN and ZigBee are some types of low-power wireless networks, which are susceptible to environmental factors such as temperature, humidity, obstacles, and human activities. These will affect communication and cause a loss of data, leading to mal-function in the data processing of smart farming systems [10].

Table 4: Overview of the functionalities and objectives of each software tool used in testing the security of the Tapo C200 IoT camera.

SoftwareTool	Functionality	PurposeinExperimentingwithTapo C200IoTCamera
Ettercap	Man-in-the-Middleattacktoolkit;breaksapartprotocols,filterscontents,andcapturesnetworkpackets	ListeninonconversationsbetweentheTapocameraand its application
Nessus	Vulnerabilityscanner;evaluatesoverallsecurityagainstknownthreatsandweaknesses	EvaluatetheTapocamera'svulnerabilities
Nmap	Networkdiscoverytool:quicklyscansnetworkstofindactivehostsandservices	Collectdataregardingtheservicesexposedbytheapo camera
SSLPacketCapture	Powerful debugging tool: interceptsencrypteddataforfurtherexamination	DecipherSSLcommunicationstoandfromtheTapo application
Iptables	Administration tool for NAT and packetfiltering;managesfirewallruleswithinLinuxkernel	Act as an active mediator between the Tapo cameraand its application, controlling network traffic andfilteringpackets as needed

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Wireshark	Transformnetworktrafficintoplayablevideoforin-depth analysis	Transformnetworktrafficintoplayablevideoforin-depth analysis

The table introduces a simple arsenal of instruments used by researchers to explore vulnerabilities in the IoT camera Tapo C200. The toolkit contains all the necessary software tools, including Ettercap for Man-in-the-Middle attacks, Nessus for vulnerability assessment scanning, Nmap for fast network scanning, SSL Packet Capture, decrypting encrypted streams of data, Iptables for managing your settings on the firewall as well as deep network packet analysis through Wireshark. These tools highlight the potential risks from the security point of view concerning the IoT cameras such as the Tapo C200 camera. Attackers will be taking advantage of vulnerabilities in encryption protocols, specifically the ones that are known to be used for Wi-Fi communications, with the help of tools like SSL Packet Capture to intercept data that is sensitive in nature in order to decrypt it and compromise user privacy and security in regard to the same [11].

Eavesdropping is a significant threat, especially to IoT devices that function within the 5G network. The shared characteristic of the spectrum in 5G is a strong vulnerability characteristic of the IoT devices. Dynamic and densely packed spectrum allocation increases the possibility of interception by a third party of sensitive data that IoTs are transmitting as a way of capitalizing on weaknesses in spectrum sharing access [12].

Table5: Various tools frequently used in Bluetooth security research and exploitation

Tool	**Function**
CYW920819EVB-02	
BBCMircobitsV2	
SemiconductorsnRF52840	

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

Flipperzero	

Table 5 depicts some of the mostly used tools in research and exploitation of Bluetooth security. The BBC Micro bit V2 outpaces the Semiconductors nRF52840 BLE as part of the Bluetooth analysis tools. These are used for multiple purposes, including Bluetooth device management and configuration, authentication fraud prevention, encryption key downgrade, human-computer interaction interface configuration, Bluetooth device scanning and identification, and applying firmware patches in real-time [13].

The majority of hacking tools used in IoT devices attacks are quite similar. For instance, Wireshark and Ettercap are used for capturing and viewing sensitive information such as passwords and login credentials of the victim [14].

Table 6: Comparisonof Wi-Fi and Bluetooth Vulnerability AssessmentSteps withFlipperZero

Step	Wi-Fi Vulnerability Assessment	Description	Bluetooth VulnerabilityAssessment	Description
1.	Power On Flipper Zero:Ensureit'sfunctional.	Ensure Flipper Zero ispoweredonand working properly.	DeviceInventory: Createadetailedlist of Bluetoothdevices..	Create a comprehensiveinventoryofBluetoothdevices in scope.
2.	Access Wi-Fi SignalCapture: Navigate tocapturefeature.	Access Flipper Zero'smenutoinitiateWi-Fisignalcapture mode.	Bluetooth Scanning: UseFlipper Zero to scan fornearbydevices.	Use Flipper Zero to scan fornearby Bluetooth devices, notingtheiraddressesand names.
3.	Configure CaptureSettings: Set channel,security,etc..	Configure Wi-Fi capturesettings including channeland security..	DeviceProfiling:Gatherdevice informationincludingversion and services.	Gather information aboutBluetooth devices includingversion,supportedprofiles,and services
4.	Start Wi-Fi Capture:Initiatesignalcapture.	Begincapturing Wi-Fisignalsbasedonconfiguredsettings	Vulnerability Scanning:Use Flipper Zero forvulnerabilityassessment.	Utilize Flipper Zero to scan forknown vulnerabilities, outdatedfirmware, etc..

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

5.	Monitor and Record:Viewandstorecaptureddata.	Monitor Wi-Fi captureprocess in real-time andstorecaptured data..	Pairing &AuthenticationAssessment:Evaluate security of pairingmethods.	EvaluatesecurityofBluetoothpairing and authenticationmechanisms.
6.	Stop Wi-Fi Capture:End signal captureprocess.	HaltWi-Ficaptureprocesswhen desireddataisobtained..	MITM Attacks: TestBluetoothconnectionsfor susceptibility to MITMattacks.	TestBluetoothconnectionsforvulnerability to Man-in-the-Middleattacks.
7.	SaveCapturedData: Store data on SD card orcomputer.	SavecapturedWi-Fi signaldataforfurtheranalysis..	ReplayAttacks:Assess resistance to replayattacks	Assess Bluetooth devices'resistancetoreplayattacks.
8.	DataAnalysis:Analyzecaptured data usingsoftwaretools.	Transfer captured Wi-Fisignaldatatocomputerforanalysis.	Sniffing BluetoothCommunication:Use FlipperZeroforcommunicationanalysis.	UseFlipperZerotosniffBluetoothcommunication

The Flipper Zero is an electronic device that scans and scans for vulnerabilities both on Bluetooth and Wi-Fi, as shown in Table 5. Open-source, adaptable hardware, it is used for ethical hacking and penetration testing on IoT devices [15]. In relation to this, PENTOS introduces itself as a penetration tester for IoT home gadgets, and such technologies are Bluetooth and Wi-Fi. PENTOS can detect vulnerabilities in wireless communication protocols, online interfaces, and password security. Based on such assessments, PENTOS does a holistic analysis of the outcome of any attack specific to Bluetooth and Wi-Fi and provides individual security recommendations that can strengthen the overall security of IoT home devices [16].

Further analysis of attempts to carry out a cyber attack on smart home environments and found identified structures of the CPU, firmware attacks were successful in extracting names and credentials from the IoT firmware images by reverse engineering, and DoS attacks can incapacitate devices within minutes [17].

4. Future Hacking Trend

IoT Device Emerging Risks Based on Wireless Vulnerabilities

The new generation of IoT home devices, with growing numbers of more and more Machine Learning (ML) and Artificial Intelligence (AI), provide both new cybersecurity opportunities and challenges. These devices come with added functionalities to malicious actors as they seem to be interested in the complexities the new technologies introduce. Some of the wireless network

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

attacks possible include:

- Adversarial Attacks on ML Models: This type of attack involves actions against machine learning algorithms performed maliciously at the training time or discovery of vulnerabilities in models leading to destructive or low-accuracy predictions.
- Data Interception and Manipulation: These attackers intercept wireless communications between cloud services and AI-enabled IoT devices to inject or alter data that goes against a decision-making process in a device.
- Privacy Breaches: The wireless vulnerabilities will compromise them to intruders, making unauthorized access to user sensitive information that has been managed by algorithms applied by AI in a certain perspective, which may lead to theft of identity or other privacy breaches.
- DoS attacks: This is where incoming traffic forwarded to a wireless network in a way that it overloads such networks or to target the communication channels used by AI-enabled devices to cause denial-of-service by preventing them from working normally and thus causing service breakdowns.
- Model Poisoning Attacks: In such attacks, malicious samples are injected into the training data of the AI model to manipulate it in uncontrollable ways.
- Evasion of Anomaly Detection: Many AI-enabled IoT devices rely on anomaly detection for security. Attackers might try to manipulate the learning process in a way that can bypass the mechanisms of anomaly detection in place.
- AI Decision-Making Exploitation: The attacker exploits decisions that might be produced by AI algorithms to get unauthorized access to systems or exploit control over other machines in the IoT environment.
- Firmware Exploitation: An attacker exploits the firmware of an AI-enabled IoT device to compromise the integrity of the device and then steal data or take unauthorized control.

5. Discussion

Most particularly, the legacy or outdated smart home hub, and because of vulnerabilities on the security update, they are most vulnerable to hackers. Serving as the central control unit of many smart devices in a house which covers communication and automation, the hubs oversee that extensive array of hardware and data. When security updates are issued by the manufacturer, older models of smart home hubs would no longer receive support, making them particularly vulnerable to exploitation.

They are most likely to be attacked on these legacy devices, often not receiving current security patches and marking the easy entry to unauthorized access across the whole smart home system. For example, a classic IoT smart home gadget with outdated firmware can have open vulnerabilities that can allow hackers to shoot for vulnerabilities in communication protocols or gain unauthorized control over connected devices. This further proves that safety within the smart home network requires periodic updates and replacements of old IoT equipment.

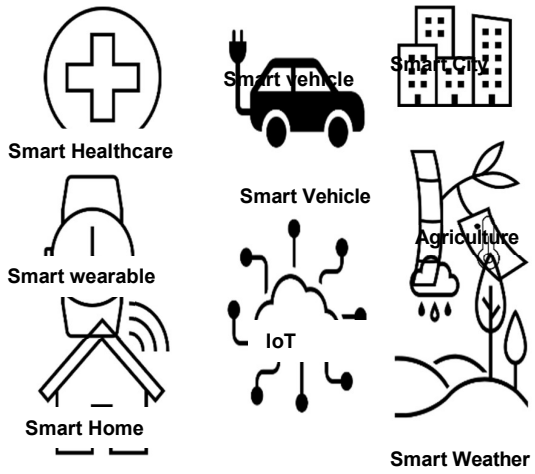
InternetofThingsHub

In the context of IoT, a "hub" would be said to mainly refer to a central device that would act as a communication gateway or control center for several connected devices in a smart home or an

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

IoT network. The hub is a central point that oversees and coordinates several interactions, especially communication between diverse smart devices, including sensors, actuators, and other IoT-enabled equipment.

Figure1: IoT applications in various fields



Security Guidelines for IoT Devices in Wireless Communication

To improve the cyber security measures for consumers using IoT devices at home, the following guidelines are provided in the table below.

Table 7: Recommendations forEnhancingSecurityofIoTHomeDevices

Recommendation	Description
FirmwareUpdatesandPatchManagement	Regular updates and patches for IoT device firmware to fix known vulnerabilities and improve overall security
User AuthenticationandAuthorization	Enhanceuserauthenticationproceduresandimplementstrongauthorizations systems storeduceunauthorized access toIoTdevices.
DataEncryptionStandards	Implementeffectiveencryptionstandards fordatatransferredbetweendevicesandnetworkstopreventinterception.
VendorAccountability	Source IoT devices from reliable suppliers, prioritizing security, and evaluate vendor security procedures to reduce risks

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

User EducationandAwarene ss	Provideuserswithinformationaboutpotentialrisksandrecommendedsecurity practicestodecreasethe likelihoodofcyberattacks.

Patching or updating the code in cases of known security breaches usually fixes the problem. Devices intended for long-term use must have the ability to update all the layers of their software to avert any future vulnerability. This table summarizes the recommendation and its description for enhancing the safety of IoT use at home [18].

It has been emphasized that identifying early warning signs of breach in piconets is crucial ,since these networks are often easy to breach. The below are glaring examples: weak PIN and dated security software running on most consumer devices' Bluetooth [19].

It is recommended thatWi-Fi router passwords be frequently renewed, as cracking WPA/WPA2 passwords takes longer time than any cracking process. Frequently updated passwords prevent illegal entry into the network and allow monitoring to block and delete unexpected access into the IoT by a device or user. Frequent security testing by the IoT product manufacturers would also help in securing their products for the safety of consumers [20].

It is suggested that, while opting to bypass certain fixes for vulnerabilities, an organization should identify such vulnerabilities in order of importance, cost, complexity, and remediation time. The Penetration testers need to rate the high-priority vulnerabilities and remedial actions using metrics [21].

The responsibility and awareness of security by consumers shall be supported through the laws, policies, and the oversight of the government. Customers should also maintain and ensure security on IoT devices and keep an eye on possible risks [22].

Conclusion

In a nutshell, it is about insight into the security of those widely used communication protocols within smart homes. This study reviews critical aspects that include authentication, encryption techniques, and the general robustness of the system and goes into detail about the risks and vulnerabilities inherent to Bluetooth and Wi-Fi-enabled IoT devices. The research is important because it adds to the ongoing discussion about how to adequately protect residential ecosystems of IoT, given the rising popularity of smart devices within homes.

It provides prospective threats and vulnerabilities to be able to help in formulating better security practices, best practices, and solutions. It underscores the very critical need to address security issues with Bluetooth and Wi-Fi-enabled devices for a smart home environment to be confidential, integral, and resilient.

This study is the first, yet crucial, step in improving the security of residential IoT systems, which will pave the way for research and development activities toward more secure solutions as this technology continues to evolve. The manufacturing community and users can utilize the information and recommendations garnered from this study in order to preserve their safety and security in the use of Internet of Things for home usage, away from cyber attacks.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

References:

[1] Nor NaematulSaadah, Ismail, and Zolkipli Mohamad Fadli. 2023. 184 International Journal of Computer ApplicationsPreliminary Review of Phishing Attacks and Countermeasures on the Internet of Things (IoT) Environment.

[2] Vikas Rao Vadi, Shafiqul Abidin "Controlling Devices by IoT", International Journal of Recent Technology and Engineering, Volume - 8, Issue – 4, N

[3] Ariyadi, Tamsir, and M. RizkyPohan. 2023. "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators." JurnalPenelitian Pendidikan IPA 9(12): 10768–75. doi:10.29303/jppipa.v9i12.5551.

[4] ***F***atima, Haram, Habib Ullah Khan, and Shahzad Akbar. 2021. "Home Automation and RFID-Based Internet of ThingsSecurity: Challenges and Issues." Security and Communication Networks 2021. doi:10.1155/2021/1723535.

[5] ***D***. Buil-Gil, J. Pacheco, and C. Romero, "The digital harms of smart home devices: A systematic literature review," *Computers in Human Behavior*, 2023

[6] ***H***eiding, Fredrik, Emre Süren, Johannes Olegård, and Robert Lagerström. 2023. "Penetration Testing of ConnectedHouseholds." Computers and Security 126. doi:10.1016/j.cose.2022.103067

[7] ***A***hmed Adbeib, Khaled. 2023. 2 African Journal of Advanced Pure and Applied Sciences African Journal of Advanced Pure and Applied Sciences (AJAPAS) Comprehensive Study on Wi-Fi Security Protocols by Analyzing WEP, WPA, and WPA2.

[8] Abidin, Shafiqul,.Vadi, VR,. Rana, Ankur,. October, 2019. On Confidentiality, Integrity, Authenticity and Freshness (CIAF) in WSN: 4th Springer International Conference on Computer, Communication and Computational Sciences (IC4S 2019), Bangkok, Thailand. Publication in Advances in Intelligent Systems and Computing pp 87-97, ISSN: 2194-5357

[9] ***S***adikin, Fal, NuruddinWiranda, JlBrigjen, Jalan Hasan Basri, Kec Banjarmasin Utara, Kota Banjarmasin, and Kalimantan Selatan. 2023. Sadikin and Wiranda-Investigation and Penetration of Digital Attacks on Zigbee- Based IOT Systems INVESTIGATION AND PENETRATION OF DIGITAL ATTACKS ON ZIGBEE-BASED IOT SYSTEMS.

[10 ***R***udrakar, Santoshi, and Parag Rughani. 2023. "IoT Based Agriculture (Ag-IoT): A Detailed Study on Architecture,Security and Forensics." Information Processing in Agriculture. doi:10.1016/j.inpa.2023.09.002.

[11] ***B***ella, Giampaolo, Pietro Biondi, Stefano Bognanni, and Sergio Esposito. 2023. "PETIoT: PEnetration Testing the Internet of Things." Internet of Things (Netherlands) 22. doi:10.1016/j.iot.2023.100707.

[12] ***R***achakonda, Lakshmi Priya, Madhuri Siddula, and Vanlin Sathya. 2024. "A Comprehensive Study on IoT Privacy and Security Challenges with Focus on Spectrum Sharing in Next-Generation Networks(5G/6G/Beyond)." High- Confidence Computing: 100220. doi:10.1016/j.hcc.2024.100220.

[13] Cook, Stephen, Royal Holloway, Maryam Merhnezad, Ehsan Toreini, and Maryam Mehrnezhad. 2024. "Bluetooth Vulnerabilities in General and Intimate Health IoT Devices and Apps: The Case of Female-Oriented Technologies." doi:10.21203/rs.3.rs-3877210/v1.

[14] Arreaga, Nestor X., Genessis M. Enriquez, Sara Blanc, and Rebeca Estrada. 2023.

ISSN:2731-538X | E-ISSN:2731-5398
Vol. 19 No. 01 (2025)

"Security Vulnerability Analysis for IoT Devices Raspberry Pi Using PENTEST." In Procedia Computer Science, Elsevier B.V., 223–30. doi:10.1016/j.procs.2023.09.031

[15] Winston James, DrJoy. 2023. Evaluating IoT Device Security: Penetration Testing and Vulnerability Assessment with Flipper Zero. https://ssrn.com/abstract=4658141

[16] Yaacoub, Jean Paul A., Hassan N. Noura, Ola Salman, and Ali Chehab. 2023. "Ethical Hacking for IoT: Security Issues, Challenges, Solutions and Recommendations." Internet of Things and Cyber-Physical Systems 3: 280– 308. doi:10.1016/j.iotcps.2023.04.002.

[17] Bhardwaj, Akashdeep, Salil Bharany, Anas W. Abulfaraj, Ashraf Osman Ibrahim, and WamdaNagmeldin. 2024. "Fortifying Home IoT Security: A Framework for Comprehensive Examination of Vulnerabilities and Intrusion Detection Strategies for Smart Cities." Egyptian Informatics Journal 25. doi:10.1016/j.eij.2024.100443.

[18] Cäsar, Matthias, Tobias Pawelke, Jan Steffan, and Gabriel Terhorst. 2022. "A Survey on Bluetooth Low Energy Security and Privacy." Computer Networks 205. doi:10.1016/j.comnet.2021.108712.

[19] Shrestha, Sunny, Esa Irby, Raghav Thapa, and Sanchari Das. 2021. SoK: A Systematic Literature Review of Bluetooth Security Threats and Mitigation Measures. doi:http://dx.doi.org/10.2139/ssrn.3959316.

[20] Md Zaglul Shahadat, Mhia, Matsive Ali, Avijit Mallik, and M Matsive Ali. 2023. An Approach on Cracking WPA,WPA2 Security of Wi-Fi with Handshake Attack. https://www.researchgate.net/publication/368241744.

[21] Sarker, Kamal Uddin, FarizahYunus, and Aziz Deraman. 2023. "Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods." Sustainability (Switzerland) 15(13). doi:10.3390/su151310471.

[22]Schiller, Eryk, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, and Burkhard Stiller. 2022. "Landscape of IoT Security."