International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I7P101

Volume 69 Issue 7, 1-18, July 2021

Original Article

A Systematic Review of Bluetooth Security Threats, Attacks & Analysis

Tahira Ali[1], Rashid Baloch[2], Mohsan Azeem[3], Muhammad Farhan[4], Sana Naseem[5], Bushra Mohsin[6]

[1]*Phd candidate & visiting lecturer, CS department Comsats University Islamabad, Abbottabad Campus, Pakistan.*
[2]*Research scholar Cs department, institute of southern Punjab, Multan, Pakistan.*
[3]*Research scholar Cs department, institute of southern Punjab, Multan, Pakistan.*
[4]*Asistent professor Cs department CUI Sahiwal, Punjab Pakistan.*
[5]*lecturer at CS Department, Allama Iqbal Open University Islamabad, Pakistan.*
[6]*Phd cs. Candidate, Comsats University Islamabad, Abbottabad Campus, Pakistan.*

Received Date: 18 May 2021
Revised Date: 21 June 2021
Accepted Date: 05 July 2021

Abstract - *Bluetooth technology is being used increasingly in electronic devices. Bluetooth is the communication medium that is most frequently used in electronic devices. Security and privacy are important, especially in communications where morbidity can have an impact. Bluetooth technology's security needs to be evaluated increasingly, particularly with devices that use Bluetooth due to the increasing popularity and use of Bluetooth embedded devices. Bluetooth sensor security has become a focus between vendors and consumers since the introduction of Bluetooth technology. The existing Bluetooth security has been extensively scrutinized and checked in recent years, and several researchers analyzed and tested Bluetooth security and raised concerns about its reliability. This study seeks to the security vulnerabilities and threats in Bluetooth embedded devices. This study addresses the major threat that affects Bluetooth Security, Bluetooth threat taxonomy, and classification and description of Bluetooth threats.*

Keywords - *Bluetooth, Security, Hacks, Vulnerabilities, Threat, MITM, Taxonomy.*

I. INTRODUCTION

Devices connected with various peripherals since the start of the computer industry. Over the passage of time, impressive field growth has resulted in a range of security measures designed to protect data transmitted through these cables. This, in effect, led to the development of security measures designed to make sure transparency, security, and dignity. Wireless networks, however, face a range of restrictions and limitations. Therefore, improvements were needed that came after the development of advanced technologies, which created new communications environments without physical interaction. The advent of wireless communications was a tipping point in the technology wheel, enabling data to be disseminated and shared in a short time. The phenomenal progress in communication and information technology has enabled the data to be Communicated instantly. Bluetooth is a commonly used networking device, particularly when it comes to mobile devices and the Internet of Things scenarios. Once a Bluetooth device is paired with a cloud device, it can then swap instructions and info/data with the present such as speech, input device or mouse, networks, user personal information, etc. Some safety measures have already been incorporated into the Bluetooth sensors, such as verification, authentication, authorization, etc., due to the sensitivity of such information and commands. Furthermore, according to previous research on the Bluetooth sensors protocol and its Android device implementation, they discover that there are even some design flaws that could run to severe safety implications [1].

Bluetooth is a technology that data to be shared in proximity between compatible devices without needing to have a physical connection. Bluetooth communication protocol creates the local adhoc networks, that is called piconets, in which connected Bluetooth peripherals communicate with each other and exchange information [2]. The device that begins a connection inside a piconet is said to a master computer, and the gadgets attached to the master are named slaves. Local ad hoc networks are dynamically active as various Bluetooth communication devices enter or leave the region of the network. Bluetooth using the Frequency-Hopping Spread Spectrum (FHSS), Bluetooth contact occurs at 2,4 GHz within the Manufacturing, Scientific and Medical band [3].

The digital identities and personal data for billions of users across the Web have been compromised in recent years by data breaches. News headlines announced in 2017 alone that criminals had hacks personal data for three billion Yahoo users, the financial specifics of 143 million Americans gathered by Equifax, and personal data relating to 57 billion Uber users [4]. Information technology is now an essential and fundamental part of industry and organization infrastructure. With the enormous growth and development of computer networks and the Internet, data traffic management and auditing are important to enhance the overall security and efficiency of a networked system. Previous studies have documented over 3.3 billion certificates arising from infringements openly exchanged on the underground of credit cards and other financial data [5]. At present, with online computer devices and the Web growing information, devices and apps protection is becoming a real challenge to programmers and managers of the devices. Most people know that online data stalking is a crime and its deal with cybercrime. While data stalking must be observed, usually harmful when the stalked information is used by an intruder for malicious reasons. But sometimes, data stalked is also used for a positive purpose.

Most of the emerging technologies currently available have dramatically improved our standard of living, and it is impossible to ignore payoffs in the sort of significant security threats. Bluetooth technology, disruptive agents can eavesdrop and compromise the integrity of communication as data is transmitted wirelessly. Intentionally, hackers can jam Bluetooth channels of communication, alter data, and even capture and retrieve confidential information.

II. BACKGROUND

The word ' Bluetooth ' arises from the nickname of King Harald Blatant of the 10th century, who was inclined to eat blueberries and unified the still-warring factions of modern-day, Scandinavian countries into a unified kingdom [6]. Moreover, Bluetooth technology is attributed to the Secret Communication System, a 1942 development patent that outlined a frequency hopping spreading range for a radio-controlled torpedo. When the radio signals constantly jumped across the continuum, the enemy was not able to infiltrate the signal and interrupt it. This patent, Bluetooth technology, did not take shape until 1994 when Swedish telecommunications company Ericsson planned to swap RS-232 cables with a wireless alternative based on radio frequency (RF) [7]. Simultaneously, other prominent corporations, such as Nokia, were considering replacing cable systems with wireless ones. The telecommunications industry felt the need to create a structured way for their divergent goods to achieve compatibility. After prolonged negotiations, a special interest group (SIG) was established in 1998, representing IBM, Erickson, Intel, Nokia, Toshiba, and launched Bluetooth technology in 1999 [7]. Bluetooth technology tends to be developed and is gaining market acceptance. It now offers many advantages, including easier sharing data, wireless sync, and Internet access. Bluetooth usage is more convenient than the technology preceding it. Unfortunately, Bluetooth technology faces several relevant threats due to its large use.

Blue-snarfing is one such threat: a mechanism in which an intruder exploits a Bluetooth connection to reach important information, such as texts, schedules, contact lists, addresses, audios & videos, and pictures. Blue-snarfing, which typically involves information and data theft, only takes place when a suspect's computer is in searchable mode [8-10]. Bluejacking is another security risk in which an attacker sends spam messages to the other Bluetooth device. Blue-jacking targets Bluetooth devices ' ability to send messages in a certain radius without the permission of the user. It is comparatively inoffensive which is often used for advertising or marketing purposes. Blue-jacking could be avoided by setting the non-discoverable mode in the device setting [8-10]. Blue-bugging is another threat, where a hacker tries to manipulate a target system and breaches its security. A trespasser uses the target device without the owner's consent through blue bugging. In addition to several other activities, the attacker can make calls, send the message, read short message service (SMS) messages and change contacts [8-10]. A denial of service is another threat that can be performed in various forms. For example, a hacker can conduct the processes of computation (e.g., send the bogus messages to the target device) structured to absorb and reduce battery power [11]. Such a battery-depleting attack is considered a sleep deprivation attack. Another type of phishing attack is a blacklist attack, triggered by decision-making during mutual authorization protocol [12].

A backdoor attack arises when an attacker is accessing encrypted information by nullifying the usual security mechanisms of a system. The attacker creates a trust relationship during the pairing process, which ensures that his or her computer does not appear in the paired devices list of the victim. Using this connection, the hacker has exposure to all data on the computer of the victim [13]. The encryption algorithms can also contain backdoors. Experts have recently described how prime numbers can be constructed in algorithm encoding so that attackers can factor the primes and crack the encryption as a result. Such risks affect all the devices with Bluetooth wireless technology [13].

III. RELATED WORK

As we have already mentioned in the introduction, the rise in popularity of Bluetooth has redirected the focus of different parties towards it, from attackers and hackers to analysts and computer security experts. A few research papers have therefore been published on the topics of both the flaws and vulnerabilities in Bluetooth technology.

This section discusses the Bluetooth security literature topic to establish a comprehensive understanding of the prevalent aspects relating to Bluetooth pairing mechanisms in the field of security issues. Extensive work was carried out to classify the various problems that may occur in the Bluetooth technology, and innumerable attacks were reported. Researchers and scientists have been actively involved in the analysis and proposing various solutions to address security issues related to Bluetooth technology. However, the ostentatious participation of prior research prompted the researchers to conduct additional research on Bluetooth technology-related security threats. Jakobsson and Wetzel invented the first MITM attack on Bluetooth, which attack version 1.0B to version 2.0 + EDR due to lack of changes to the authentication specification. The attack model suggests the two Bluetooth gadgets and the intruder are located in a circle in which the hacker is aware of the connection key used in both two devices. Jakobsson and Wetzel also described other vulnerabilities which resulted in further attacks being formulated. The first assault decides the device's current location, and the second concentrates on the cipher. However, the researchers explained the method of retrieving the connection key to use an offline PIN rustling attacks by passive eavesdrop at the authorization key protocol [14].

Later, Gehrmann, C. & Nyberg, K. [15] presents the issues posed in [14] by adding an authentication mode to escape geolocation. The researchers also explained that via Bluetooth Baseband Security, convenient and secure access point roaming could be accomplished by extending the existing link key aspect and using the improved key pairing mechanism. In that same narrative, Kugler [16] enhanced the incursion proposed in [14] by demonstrating that by altering clock settings, the hacker can compel equally target devices using the same channel-hopping pattern with distinct clocks. The two victim systems are thus unsynchronized, and the attacker can only access the texts sent to them. Kegler also defined how to conduct a MITM attack during the scanning process. Specifically, a hacker who can react to a victim's request for a page faster than a slave victim can reboot the slave's paging

procedure with a different clock [17]. “Singel´ee, D. & “Preneel, B”. [17] also indicated that system keys should not be used, as keys were stored in un-variable memory and rarely modified. [17] discovered that an attacker might manipulate the random number and, in effect, the PINs and passwords in the initialization stage. With reference to the vulnerabilities raised by [14] and [18], [19] suggested the need for an improved key exchange Diffie Hellman that optimized security through a one-way cryptography feature. The authors also suggested the use of user-friendly PINs with parameters from 5 to 12 and also an ECDH in the next edition. This proposition was intended to stem hose-tapping and offline attacks. In addition, Bluetooth SIG identified that Protected Wireless Protocol was both vernacular attacks both by an internal and external approach, so they suggested changing the size of the PIN.

Another form of attack, the reflective attack (relay), contains a victim's device being impersonated [19]. A reflective assault can be one-sided so that one target device is impersonated or two-sided to impersonate both target devices. In addition, no need for the hacker to acquire any confidential information in a reflection attack because the hacker relays the information gained during the verification process from one targeted system to another. These attacks only require the victim’s devices ' Bluetooth Device Addresses (BD ADDRs). However, the attack on reflection could be viewed as a form of MITM threat against authorization rather than encryption [19]. Sayegh, A. A. & El-Hadidi, M. T. [20] discovered dictionary attacks and suggested the use of BT-EC-SRP protocols which effectively generates a secure authorization key. Giousouf, A. and Lemke, K., [21] demonstrated many Bluetooth drawbacks, including the short PINs and the vulnerability of key unit sharing to eavesdropping attacks. Bluetooth also lacks processes to verify device addresses, so hackers can manipulate addresses. In addition, Bluetooth is suffering from restricted security capabilities, a deficit of end-to-end encryption, a poor E0 streaming cipher algorithm, a tradable key duration of encryption, a lack of reciprocal authentication, and an unknown strength pseudorandom challenge answer generator. Shaked, Y. and Wool, A., [22] described the benefits of a short PIN and described the attack in which the hacker can found and decode the PIN used during the pairing process quickly and easily.

An attack on Bluetooth 2.1+EDR key Access Mode is defined in [23] and techniques developed in [24]. In this attacker uses the Passkey Entry's design vulnerabilities, particularly during stage 1 authentication. For an attack should be successful, it is essential to reuse the passkey in a second effort at pairing. The attack is based on two principal measures. First, during an SSP operation, the attacker fixates on two authorized devices and then monitors all messages transmitted during verification stage 1 and the actual DH exchange. The hacker then blocks the communication channel and interrupts the session with the SSP. The hacker impersonates systems A to B during the second step by triggering a new pairing phase and storing the same key previously used between the two legit devices. In this case, the hacker functions as MITM and uses the key to negotiate and authenticate connection keys. The hacker will ultimately manipulate the data shared between the two authorized devices. It is important that in future verification procedures, even if the second device is missing, the hacker may imitate one device to the other due to the reuse of the connection key. The vulnerabilities in SSP arise to another means of attack conducted on Bluetooth versions 2.1 or later, in which either the attacker induces victim devices using the JW association model or invalidates I / O information during SSP's first step.

Haataja and Toivanen have invented two new MITM attacks on the Bluetooth SSP [25]. The first attack forges the information on I / O abilities during SSP's first stage. In the second attack, the hacker creates sensory communication with the victim system to confuse the user and encourage the user to choose a less reliable model rather than a more reliable model. The attack is designed to be the most efficient way of avoiding MITM attacks, demonstrates only a semblance of the existing dangers crawling in the latest security improvements. Many new Bluetooth users can easily switch their Bluetooth client address and deliberately uncover Bluetooth devices which cannot be discovered [20]. This indicates that MITM attacks affect all four SSP alliance models, and danger is growing in relation to Bluetooth technology's popularity.

In [26], a first step was taken by the authors in automating the study of structured aspects of human authorization protocols. They showed that authorization could fail if the same system is involved in recurrent Simple Pairing sessions. The authors optimized the authorization scheme by adding session identifiers and showed that the new authorization model preserved Simple Pairing's authorization properties.

Das, A.K., et al. [27] reported a greater risk of personal data breaches from Bluetooth Low Energy (BLE) apps, such as health trackers. The attack scenarios, which exploited BLE devices, were introduced in [28] and expanded in [29]. Because attacks on BLE systems are based on packet sniffing during the pairing process, the researcher exploited the weakness of BLE pairing. They compare this with another framework, the Fitbit Flex, which uses a different passkey protocol for extra protection known as the ANT protocol. They also demonstrated how to crack a traditional BTLE pairing with open-source software with ease [29]. An article in [30] recently reported an attack called the Blue borne attack, which hops from the Bluetooth device to the Bluetooth device within the range. Mutchukota, Saroj, and Sanjayin [31] discuss Bluetooth vulnerability and MITM attacks and discuss initially proposed countermeasures for Bluetooth SSP MITM attacks. Scarfone, K. and Padgette, J., in [32], has been written as a tutorial discuss the important aspects to know about the security of Bluetooth technology. This provides details on the pairing process's current capabilities and gives feedback to organizations that should engage in improving existing standards. This is specifically important when it takes to evaluate the effectiveness of countermeasures provided in all versions of Bluetooth from 1.0 to 4.2.

IV. METHODOLOGY

we focus on relevant and important Bluetooth security issues. To do this, We examined systematic reviews of Bluetooth Security: Threats, Attacks & Analysis screening publications to identify the relevant literature. The databases are searched to identify relevant studies using the following search strategy:

Research Query: Bluetooth AND Security AND Hacks AND vulnerabilities AND Characteristics (methods OR techniques) AND Targets AND Cyber AND Threat AND MITM AND attacks AND Taxonomy AND Severity AND (equipment and supplies) OR device.

Selection of reviews

This section reviews for the systematic analysis were included if they met the following inclusion criteria:

- The review paper addresses the comprehensive understanding of the Bluetooth pairing mechanisms in the field of security issues.
- The review paper identifies the various problems that may exist during the Bluetooth communication process, and multiple attacks were documented.
- The review paper addresses the significant contribution of previous works that prompted the researcher to conduct additional research on Bluetooth pairing mechanisms related to security issues.

A. Screening and data extraction

Duplicates were deleted from the search results. If they were guidelines, were no longer accessible online, or were in a language other than English, the article was also excluded. Three investigators separately screened the titles of the article and the abstract against the criteria for inclusion and then examined the full text of the articles against inclusion and the criteria for exclusion. Analyzed the types of primary research, analyzed the collection of outcome tests, the absence, and existence of meta-analysis. We have left out those posts that had no address the above-mentioned criteria.

a) Analysis

The search brings up 558 pieces of kinds of literature from which the inclusion requirements were fulfilled by 10 research papers.

B. Summary systematic review characteristic

For 872 publications 104 have been omitted due to duplications. The inclusion requirements were met based on the titles and the abstract review of Articles 336, then 311 were omitted. Articles 25 had been included to access the full text, and then only 10 articles met the criteria.

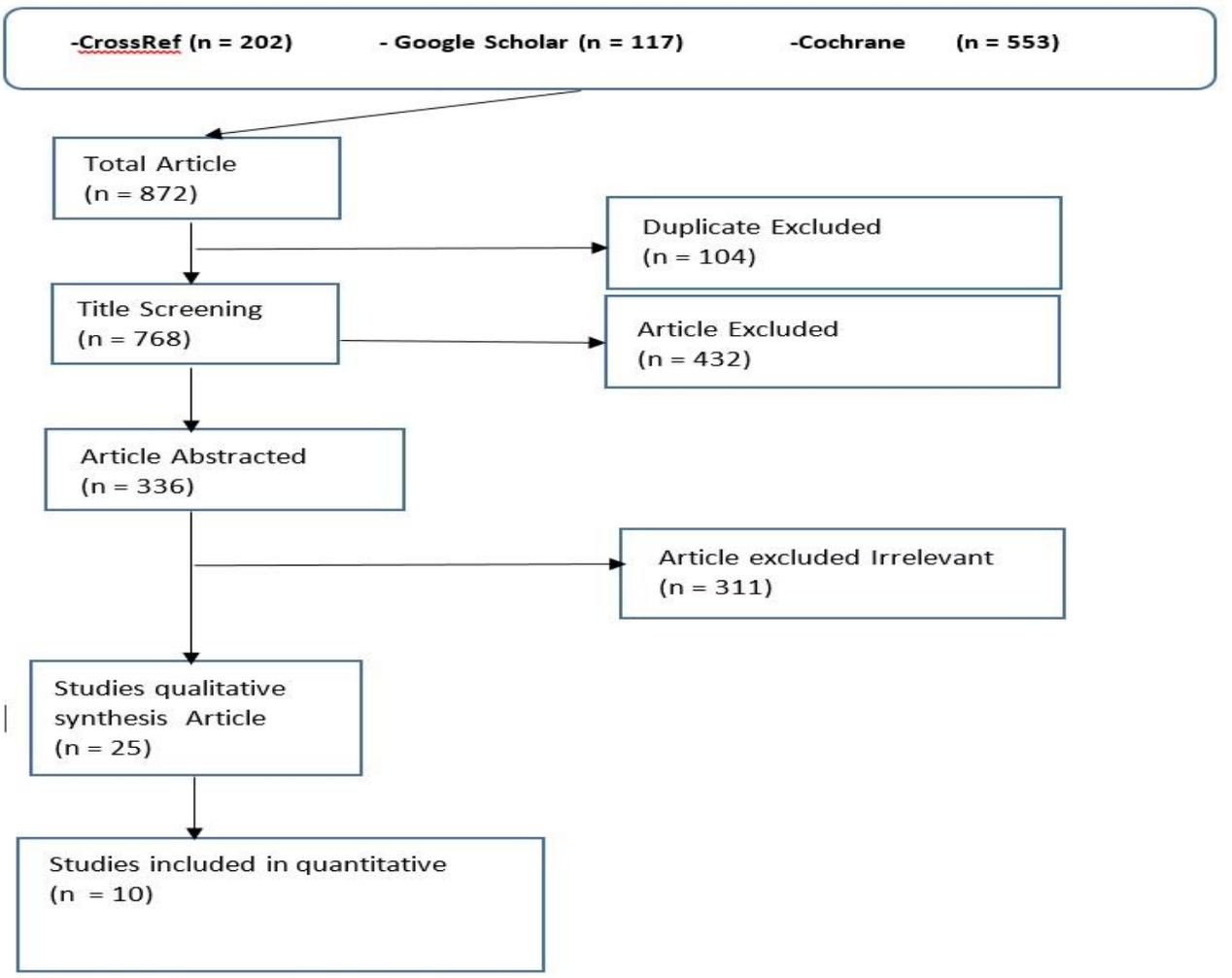

Fig. 1 PRISMA flow diagram of studies' screening and selection

Table 1. Systematic review paper

sr. No.	Year	Paper Title	Author	Publisher	Purpose	Findings
1	2009.	Bluetooth hacking A Case Study	Dennis., Browning, Gary C. Kessler	Journal of Digital Forensics, Security and Law,	This article explains an undergraduate project that examines mechanisms for attacking devices enabled by Bluetooth. The paper explains the Bluetooth procedure architecture and Java (Gui)that can be used by programmers to connect to Bluetooth data communication services. In addition to a comprehensive description of two attacks methods, (Bloover) II and B.T Info are listed.	This project's goal was to decide how serious the risk of Bluetooth-enabled devices attacks is and how quick it is to launch such attacks. The main examples of Bluetooth's risks are the possibility that someone could listen to all the conversations a person has without them understanding them or getting their text messages to read. Even worse, without the victim even realizing, an intruder may initiate a call or text to someone. Users need to be informed of these devices ' limitations so they can use them more reliably, safely, and with greater confidence.
2	2012	Security Risks in Bluetooth Devices	Vinayak P. Musale & S. S. Apte	International Journal of Computer Applications	The study discusses the critical issues found in all Bluetooth-enabled devices being tested and the threats reported. The study will also clarify what Bluetooth is, how it operates, and some of its related drawbacks and threats.	Bluetooth is a relatively stable WPAN protocol that still has flaws in its security architecture, make it vulnerable to attacks by unauthorized intruders and the risks associated with their uses. With wireless technology, the most major risk is that the core messaging medium is available to everyone, including both legitimate users and intruders. For example, if the attackers had the frequency to connect to your PC, they might use their own Bluetooth software to track and control the mouse. So they can have all of your PC's data. Via wireless connections, malicious actors may obtain unauthorized access to the computer network of an entity, bypassing any firewall security. The study suggests Wireless systems cover all of the flaws that cover a traditional wired network.
3	2014	Bluetooth Technology: Security Issues and Its Prevention	Vikethozo Tsira & Gypsy Nandi	Int.J.Computer Technology & Applications ,Vol 5 (5),1833-1837	Bluetooth technology becomes popular, and there are growing weaknesses in its protection that can be very risky to the personal details of users. This research describes the malicious intrusion on computer attacks when connecting to other devices using Bluetooth software during data sharing. It also addresses different security mechanisms that can be used with Bluetooth technology during data sharing.	In this study, Bluetooth could lead to computer vulnerabilities and loss of data by the following methods: MAC spoofing attack, Cabir Worm, BlueJacking attack, BlueSnarfing attack, Blue over the attack, Fuzzing Attacks and Backdoor Attacks and suggest Bluetooth Safety Checklist with guidance and suggestions to create and maintain Bluetooth Safe. The study suggests designing a wireless security policy, Bluetooth users are aware of their responsibility for protection, Bluetooth devices should be set to the lowest power rate, PIN codes that are sufficiently random and lengthy, antivirus needs to be enabled.
4	2016	Bluetooth	U.L.Mu	International	Many phones now use this	This paper provides an overview of

		Security Analysis and Solution	hammed Rijah, S.Mosharani, S.Amuthapriya, M.M.Mufthas, Malikberdi Hezretov, and Dhishan Dhammearatchi	Journal of Scientific and Research Publication, Volume 6, Issue 4, April 2016.	Bluetooth technology to communicate, the possibility of security problems is high. The paper would concentrate on Bluetooth, its associated vulnerable threats, Bluetooth-related network securities, how it operates. Through this study, the solution to vulnerability issues will be addressed through presenting various security tips and feasible solutions, such as holding security seminars and also doing some workshops for the device user.	some of Bluetooth's big attacks along with some potential solutions over the years. There have also been some security tips provided to users to build instant awareness among them to be more vigilant about their significant personal data. The risks are higher if an engineer in this sector ignores the security threats.
5	2017	Security threats in Bluetooth technology	Shaikh, Hassan, Soumik Das., Bibon, M. Shohrab Hossain.,M. Atiquzzaman	Computers & Security, 74, pp.308-322.	In this report, a systematic survey was conducted to recognize and explain major security risks in Bluetooth communication. While manufacturing companies of Bluetooth devices are performing their part to maintain the equipment safely, users should be informed of these risks to security and take the least possible precaution. The aim of this article provides a comprehensive study of Blue-tooth technology's potential threats and to propose possible solutions.	This paper findings, Most of the Bluetooth attacks in this paper results go undetected or unreported. The biggest advantage of a hacker would be the absence of concerns about threats to the Bluetooth. Users will stay safe with a little information about these risks. This study will help scholars find new kinds of risks that are still unidentified via awareness of these current threats and further examination, as well as potential exploitation combinations. Bluetooth devices ' research and development teams will focus on these risks and progress improved built-in safety procedures for their phones. In this study, numerous Bluetooth attacks have been grouped together that can be useful for vendors to build results that can defend against similar groups of assaults. There is no specific product in this study to avoid Bluetooth Denial or Services (DoS) attacks. This study may provide information and encouragement to develop a product in Bluetooth technology to avoid “DoS” attacks. This research suggests improving the Bluetooth architecture application layer for improved sharing of link keys and coupling device authentication.
6	2019	Analysis on Bluetooth Security	B. Chandan, R. Anand, K. Shradha Raj, R. Jeevith, Venkatesh	International Journal of Research, in Engineering, Science and Management Volume-2, Issue-5, May-2019	Bluetooth embedded devices have security vulnerabilities similar to any other wireless security. Instilling awareness of security and applying protective measures, the liabilities of both gadget producers and users, are critical to avoid dangerous	We examined BT security and the most common attack procedures in this paper: BlueSnarf, BlueSnarf++, and BlueBug. BT service users should follow good practices, such as turning off BT when not using it, limiting BT settings, removing trustworthy devices when no longer required. Moreover, BT devices provide a safety barrier that protects their

			Bhat5		violations of safety measures that could involve data and financial loss as a result of identity theft.	consumers by default, rather than depending on them to pursue good practices. In Bluetooth Networks, the use of digital signature and authentication through a trusted third party is seen to improve security.
7	2018	An Active Man-in-the-middle Attack on Bluetooth Smart Devices	Tal Mela Med	Safety and Security Studies, p.15.	This study addresses the key security issues in the Bluetooth Low Energy protocol (BLE) and explores a potential framework for BLE Man-in-the-Middle (MitM) attacks in combination with the appropriate equipment. Furthermore, a case study focused on their use was provided after presenting some of the existing tools for hacking BLE, explaining a MitM attack between a Wireless smart device and its associated smartphone app.	The study article confirms that BLE against passive eavesdropping is insecure and vulnerable. A study has shown in particular that passive eavesdropping can effectively become an effective MitM intrusion that allows a potential hacker not just to listen to correspondence but also to capture and manipulate information. In addition, in a case study described in this report, it has been shown that hackers can even monitor and control the mobile device used to connect with the Wireless smart device by executing a MitM attack in some instances. It should be noticed that Bluetooth Module Configuration v5, recently launched by Bluetooth, adds additional protection and security-related features. Given these significant improvements in BLE Safety, it is important to be mindful of and fully understand the limitations of the smart devices we use instead of depending on them blindly.
8	2018	BadBluetooth: Breaking Android Security Mechanisms via Malicious Bluetooth Peripherals	Fengha o Xu, Wenrui Diaoyz, Zhou Lix, Jiongyi Chen, Kehuan Zhang.	Network and Distributed Systems Security (NDSS) Symposium	This study's findings were on both the Bluetooth protocol and its Android device implementation. This research addresses design flaws and vulnerabilities in Bluetooth devices, which could lead to severe safety consequences.	In this analysis of the Bluetooth profiles, four development vulnerabilities have been found, which are 1) Unreliable Profile Authorization Process. 2) Profile Connection Openness. 3) Ambiguous and deceivable UI. 4) No Profile Permit Maintenance. Further attacks to show the viability and potential damage of such vulnerabilities on Android, including data theft, device control, system sniffing, voice command insertion. In addition, this study assumes that these newly discovered vulnerabilities are not restricted to a particular version of the OS. Wide versions of Android are unstable, ranging from 5.1 to the new 8.1, and similar issues may also occur on other OS platforms. Such shortcomings are embedded in the Bluetooth stack's commonly incorrect understandings and assumptions. This study suggests that a comprehensive security review of the Bluetooth protocol is still needed.
9	2019	The KNOB is Broken: Exploiting Low	Daniele Antonio li, SUTD;	28th USENIX Security Symposium	The Key Bluetooth Negotiation (KNOB) attack is discussed in this article. This attack will reduce the	KNOB attack implementation allows checking if any system accepts a 1-byte entropy encryption key (N = Lmin = 1). After carrying out the

		Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR	Nils Ole Tippenhauer, CISPA; Kasper B. Rasmussen,		entropy of any Bluetooth BR / EDR link to 1 byte of the encryption key. Bluetooth's specifications provide an unstable encryption key negotiation protocol that supports entropy values between 1 and 16 bytes. The hacker essentially violates Bluetooth's security guarantees without having to have any hidden content.	KNOB assault effectively on more than 14 separate Bluetooth chips (attacking 21 different devices). This study concluded, based on observations, that there are no discrepancies between the design and implementation of both the Bluetooth controller and the Bluetooth host and can be used as a Bluetooth user interface. The KNOB assault is a serious threat to all Bluetooth users ' security and privacy. This article, Explore these fundamental issues in a commonly used and 20-year-old standard. This research encourages Bluetooth to review the Bluetooth standard based on our results. We do not suggest trusting any network-layer encrypted BR / EDR link until the specification is set.
10	2019	Tracking Anonymized Bluetooth Devices	Johannes K Becker, David Li, and David Starobinski	Proceedings on Privacy Enhancing Technologies; 2019 (3):50–65	This investigation presents an address-leftover algorithm that develops the asynchronous presence of load and speech alterations to track beyond a device's address randomization. Further define an identity-exposing attack through a phone adapter that allows persistent, non-continuous monitoring, as well as an iOS side platform that allows user activity insight. In the context of Bluetooth advertising, provide countermeasures to the presented algorithm and other privacy flaws.	Most desktop and smartphone operating systems enforce address randomizations by default but established that devices running Windows 10, iOS, or macOS frequently share advertisement events with other BLE apps. The address-carryover algorithm explores the transient complexity of the switch in report and load and uses an unaffected identification token in the payload to find a known computer a new incoming random email. On Windows 10 and sometimes on Apple operating systems, the algorithm is consistently successful. The corresponding identification tokens switch out of step with the commercial address in both situations. Any system that frequently advertises information containing acceptable tokens will be susceptible to the carry-over algorithm if it does not synchronize all its identification tokens with the advertisement email. This concern for privacy is amplified by the practical possibility of BLE-based botnets and related threats such as vast-scale user monitoring through insecure Wi-Fi routers, which expand tracking capabilities to a global level.

V. FINDINGS

This study aims to discuss the security and privacy issues of users when using Bluetooth devices. Based on it, the question arises of how the manufacturing of Bluetooth sensors can improve the safety of Bluetooth embedded devices. Looking at the existing Bluetooth security landscape, the major research issue becomes:

Main Research Question: What are the security vulnerabilities and threats in Bluetooth embedded devices?

This research question is narrow and incorporates all consumers who used Bluetooth Devices. To answer the main question, we have to break the main question into several sub-questions.

RQ1: What is the major threat that affects Bluetooth Security?

RQ2: Classification and description of Bluetooth threats.

RQ3: What are the taxonomy for Bluetooth threats.
RQ4: What are the security issues that can become the cause of Bluetooth security unsatisfactory?
RQ1: Major threat that affects the Bluetooth Security
Bluetooth technologies are used today in millions. Those devices are subject to various kinds of threats. Bluetooth security strategies must evolve continuously to minimize emerging threats. Bluetooth signals can be intentionally interrupted or disrupted as any other wireless communication network. The unauthorized users can send incorrect or modified details to the computers.
Bluetooth security threats can be classified into three main categories as follows [33]

- Disclosure threat: The details can lead to an eavesdropper from the target system that is not allowed to access information.
- Denial of Service (DoS) threat: Users may be allowed to access service by either processing it unavailable or limiting its accessibility to an authorized customer.
- **Integrity threat:** The details may be changed intentionally to confuse the receiver.

There are following Bluetooth attacks are written below [33]

A. Man-In-The-Middle (MITM) Attack

The first MITM invasion of privacy was produced on the concept that the hackers understand of the Bluetooth devices shared key used. Certain techniques like eavesdropping and brute-forcing, the PIN can also be used to get the connection key. A hack that uses Bluetooth clock manipulation requires devices that on separate clocks use the very same hopping chain. You may achieve a hack by addressing the master device's page question instead of the slave. Using a separate clock, it restarts paging with the worker. Throughout Safe Simple Pairing (SSP), MITM attacks may be launched. Once the hacker (MITM) has a visual connection to the devices of the victim, the attacker acts before the legitimate user to create Bluetooth links to the devices of both victims and to begin the process of IO in which the less secure association model may be selected with force [34].

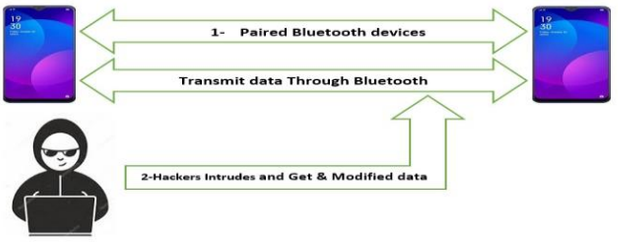

Fig. 2 Man-In-The-Middle (MITM) Attack

B. MAC Spoofing

Spoofing is performed before encryption and when creating the piconet. By producing link keys, devices can authenticate one another. The assault is continuing, although attackers may impersonate an alternative customer. An attacker may terminate the connections or change data during communication using certain spoofing tools [35].

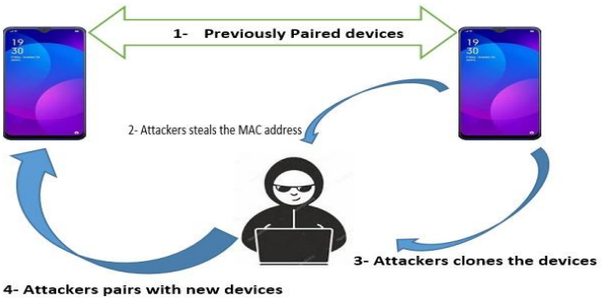

Fig. 3 MAC Spoofing

C. Blue smack Attack

A Blue smack attack is the equivalent of the Ping-of-Death denial-of-service attack in Bluetooth. It is the buffer client overflow problem that uses L2CAP messages, which includes a large number of packets sent to the survivor node in a short time interval [36].

D. Blue Bugging Attack

Blue bugging might be a very alarming threat. The attacker gets unlawful access to a device in a blue-bugging attack and can run commands or perform other actions like making phone calls. Such actions can lead to big problems. Blue bugging implements a security problem in the software of some old Bluetooth devices (often those that use Bluetooth classic) to obtain access to the system and its instructions. Blue bugging can be prevented by removing Bluetooth radio functionality while not in operation, as only when Bluetooth is allowed will Blue-buggers link. A check of all received interactive communications for viruses is also beneficial. Blue-buggers often get access to the system by giving it such details [37].

- A hacker can activate calls by phone.
- The call may be placed by an intruder.
- An intruder would be able to control phone calls.
- Could an intruder send text messages?
- An intruder would be able to read text messages.
- An intruder may connect to the internet and have the computer vulnerable to malware intrusion.
- An intruder will access the service of the Global Positioning System (GPS) and track the victim's location.
- An intruder can edit a phone book, files, calendar, etc.
- All device settings can be reset by an attacker.
- An attacker can obstruct and paralyze a network operator.

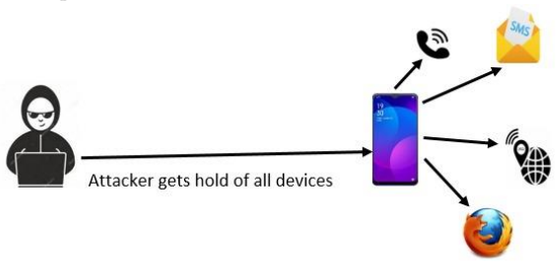

Fig. 4 Blue bugging attack

E. Blue-Snarfing Attack

Blue-Snarfing allows connecting to a Bluetooth node unapproved. The hacker exploits the node in this attack in order to gain access, the contact book, text data, etc. It might also transfer messages and calls to another device [38]. Blue-Snarfing can be prevented by deactivating the device's exploration mode, leaving the system in an unseen mode, and using software that limits computer access to only identified users.

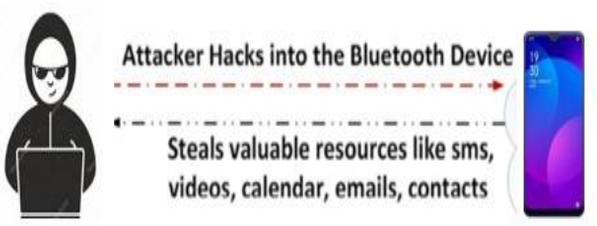

Fig. 5 Blue-Snarfing attack

F. Blue-Printing Attack

Blueprinting is a technique of extracting information from devices enabled by Bluetooth remotely. Blueprinting may be used to generate manufacturer and model statistics and to determine whether Bluetooth security devices are available in the range. Safety standards include turning off the Bluetooth function when not in use, using encryption and authentication when necessary, and then never pairing with an unidentified device.

G. DoS Attack

In a Denial-of-Service (DoS) attack, the hacker tries to discourage authorized users from accessing the service by giving the Bluetooth device a very large number of messages. Denial of web attacks may be aimed at destroying the Bluetooth device's battery power through the repeated operation. An attacker may, for example, send frequent pairing requests or requests for device information to a Bluetooth device. This continuous activity consumes the device battery quickly and results in a DoS attack that drains the battery [39].

H. BD_ADDR Attack

The attack happens when a ' bug ' is held inside a Bluetooth gadget's coverage area. The bug copies destination device BD ADDR. It should be noted that the address of the Bluetooth Device (or BD ADDR) is a unique, 48-bit identifier assigned by the manufacturer to each Bluetooth device. When a Bluetooth node tries to connect to the target device, both the bug and the target device simultaneously react and create jamming. This gives the actual valid user a lack of access.

I. SCO/eSCO Attack

This assault is focused on a two-way speech packet in real-time. It gets a lot of attention from a Bluetooth piconet, so genuine piconet devices can't access the service within an agreed time frame. Developing an enhanced SCO (e-SCO link) with piconet master may lead to this attack easily.

J. L2CAP Guaranteed Service Attack

The attacker asks for the highest bandwidth performance and lowest latency. This results in rejection of all the other requests as bandwidth are also now completely reserved for the attacker [40].

K. Fuzzing

This interference means sending malformed or any other un-standard data to the Bluetooth radio of a computer and monitoring how the system is reacting. When these attacks slow or stop the answer of a device, this means that there is possibly a significant flaw in the protocol stack [41].

L. Blue-Borne

This threat helps an attacker to take advantage of vulnerable Bluetooth frameworks on all other platforms (Linux computers, Amazon, Google Home devices, and Android devices) to remotely access or obtain information [42].

M. Multi-Blue

An attacker will reach the node that is to be breached in this attack. A Bluetooth-compatible 4 GB thumb drive, the Multi-Blue dongle is used to keep control of the target device. The attacker enables the use of the Multi-Blue program to submit requests for matching to searchable nodes. The intended computer then provides a token (a pre-shared key), which is used as authentication key by the Multi-Blue program. Then the attacker has full control of the nodes [35].

N. Cabir worm

The Cabir worms are malware that looks for accessible Bluetooth devices and transfers themselves to them using Bluetooth technologies. To hack the phone, the consumer has acknowledged the worm manually and activate the malware. The Mabir worms are basically the modern version of the Cabir worm that replicates Bluetooth and the Multimedia Messaging Service (MMS) messages.

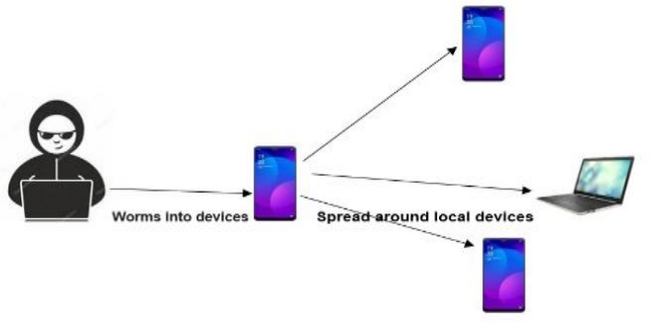

Fig. 6 Cabir worm

O. Helemoto

This assault is just like the Bluebugging attack, but on other devices, it targets the weak execution of a "trusted phone" management. As it is with Bluebugging attacks, the intruder pretends to submit a Virtual Contact File (vCard) on the victim's device to an unconfirmed Bluetooth Object Exchange (OBEX) Push Profile. The OBEX is the Bluetooth specification profile that allows a Bluetooth device to transmit an object (file) together with another Bluetooth device. Once the attack starts, the attacker interrupts the process of transferring, and the victim lists the phone of the attacker as a trusted instrument. The intruder then links up with the victim's device and gives AT instructions [36].

P. Free Callings

The attacker exploits the Wireless device of survivors and pairs a headset to a Bluetooth system which makes a free phone call. This assault causes the victim financial damage, as the survivor has to pay the call bill. Besides that, the intruder will listen to the victim's talk using t hat headset.

Fig. 7 Free Calling

RQ 2: Classification and description of Bluetooth threats

The Bluetooth consists of nine separate Bluetooth-related threat classifications. Specific classifications of the attacks require different levels of threat. For example, Monitoring and range-extension techniques may be considered benign if not combined with the more major attacks like UDDA and MITM. Threats from Bluetooth groups to promote a greater understanding of the existing and zero-day assaults. The level of threat relies on the possible harm caused by the assault. To understand fully the Bluetooth threats, one of them must have significant knowledge of the innovation. The Bluetooth discussion provides knowledge into the clarity of performing many of the listed Bluetooth Attacks. A large number of these tools for attacking are available freely, and anyone can use them. Training with these devices provides visibility into the major threats they face. Application of the information obtained in the same context by hazard analysis may provide information into identification and analysis of evolving threats. Through getting a better understanding of these threats, stronger protections may be designed to minimize their damage.

Classification	**Threat**	**Description**	**Threat level**
Surveillance	BT scanner, Bluescanner, Bluefish, Blueprinting, Redfang	Its principal objective is to collect information; to facilitate the use of certain tools.	Low
Man In The Middle	BT-SSP-Printer-MITM, Bluespoof	MITM assaults are easier to perform on computers utilizing Security Mode 1 or Security Mode 4 setting to JustWorks. Such attacks are risky because they breach security and gaining access to all transmitted data.	High
Denial of Service	Battery exhaustion, signal jamming, BlueJacking, Blueper	Bluetooth is almost never used for sensitive contact; the loss of those channels of communication attributable to DoS mostly contributes to pure confusion and irritation.	Medium
Range Extension	Bluesniping	The main objective is to provide a protected range for an intruder to launch attacks.	Low
Fuzzer	Bluepass, Bluesmack, BlueStab	Bluetooth is often not used for sensitive contact, and Fuzzers often only cause frustration and confusion when those connectivity networks breakdown	Medium
Obfuscation	Spooftooph , Bdaddr	The primary aim is to cover the attacker's identity	Low
Sniffing	Merlin , Bluesniff , Wireshark , Kismet	Sniffing may be helpful in retrieving data from unsecured communication (which is used by some devices by default), although it is most often encrypted.	Medium
Malware	BlueBag, Caribe, CommWarrior	Such attacks may be effective when it comes to harmful behavior, but the vast array of Bluetooth devices restrict their danger to a few devices.	Medium
Unauthorized Direct Data Access	Helomoto, Bluebug, Bloover, BlueSnarf, BT crack, Whisperer	This group is perhaps the most negative because of the frequency of some assaults and the severity of the stealing of data.	High

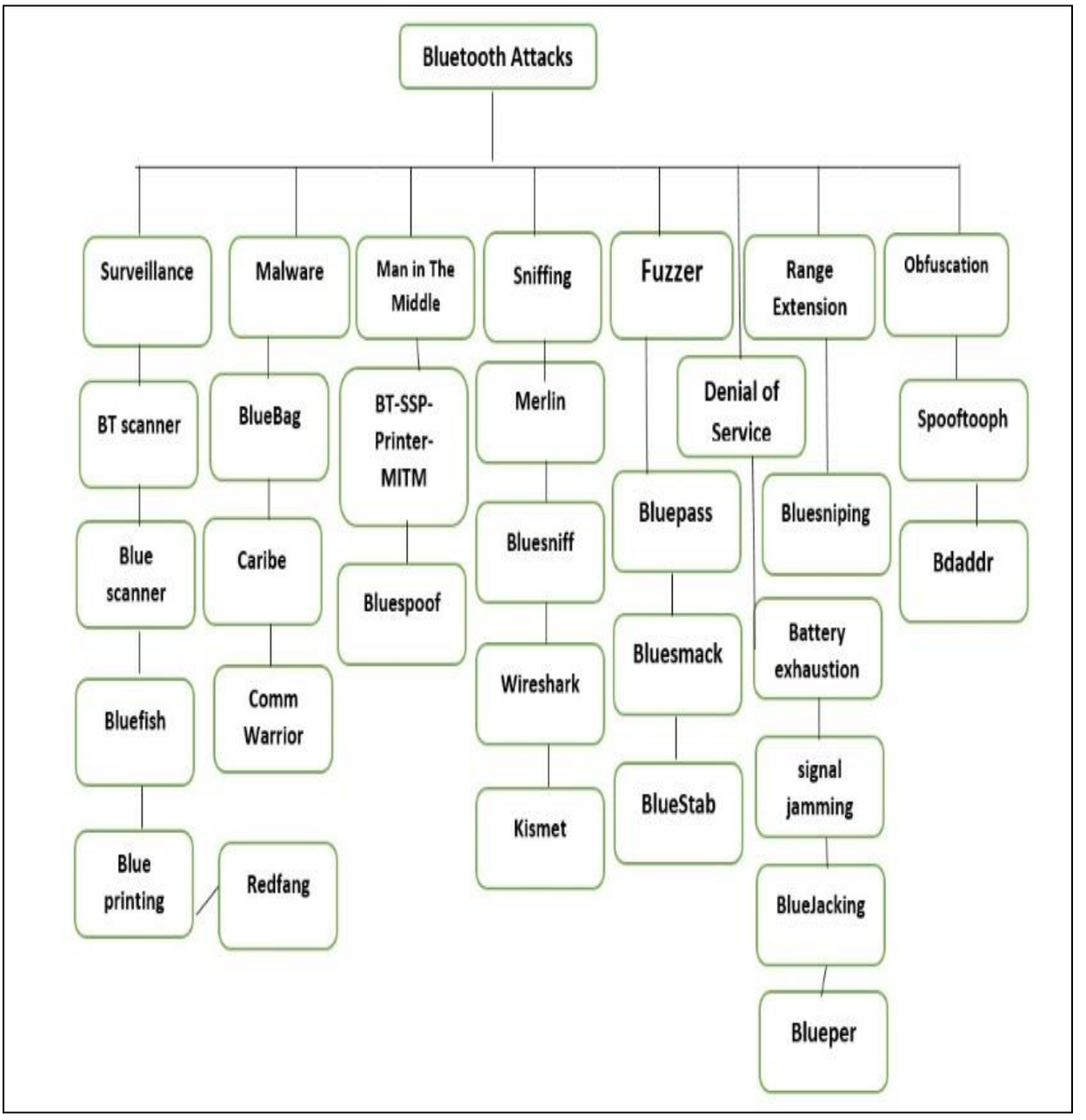

Fig. 8 Classification of Attack

RQ 3: Taxonomy for Bluetooth threats

The right to freedom of speech of privacy, and secrecy are essential components of Bluetooth devices. Privacy is a major issue like any type of data exchange technology. With all security features discussed, there have been increasing numbers of threats designed to exploit security issues in Bluetooth technologies. Such attacks cover the entire Bluetooth security strategy from the installation of applications, system configuration, messaging services, and even design. The Bluetooth Threat Taxonomy (BTT) provides just a framework for classifying all threats based on Bluetooth. The classification of attacks can help determine the intensity of the threat, precautionary methods, and reactionary strategies. Understanding fundamental differences in threats of the same classification may help to apply prior knowledge to the new threats. It is the first taxonomy for classifying Bluetooth attacks to the awareness of this author. Bluetooth Threat Taxonomy is made of nine separate classifications. Many of these categories are already common Cyber Security jargon [43]. There are following classifications by Bluetooth Threat Taxonomy: Surveillance, Malware, Sniffing, Obfuscation, Denial of Service, Range Extension, Unauthorized Direct Data Access, Man-In-The-Middle, and Fuzzer.

Table 3. Taxonomy for bluetooth threats

Classification	Methodology	Threat
Obfuscation	Methods are used which eliminate identification and hide each attack.	SpoofTooph
		Bdaddr (Device Address)
		BTClass / HCIConfig
		HCIConfig
Surveillance	Surveillance of devices to gather information.	Redfang
		BlueScanner
		BlueProPro / BNAP BNAP
		Bluefish
		War-Nibbling
		Bt Audit
		Blueprinting
		Sdptool
		HCITool
Range Extension	The connectivity range is lengthened so that attacks may be carried out remotely.	Bluetooone / BlueSniping
Sniffing	Packet capture is used to record network activity to capture data.	Merlin
		HCIDump
		BlueSniff
Man-In-The-Middle	Attackers manipulate devices into believing that they are matched when both are in reality linked to the attacker.	Bthidproxy
Unauthorized Direct Data Access	Datastore in the cloud is accessed directly due to deficiencies.	Blooover / Bluesnarf
		Btpincrack/ BTCrack
		Car Whisperer
		Btaptap
		HID Attack
		Bluebugger
		HeloMoto
Denial of Service	Things are interrupted, rendering a computer or network inaccessible for consumers.	BlueSmack
		Blueper
		BlueSpam /BlueJacking
		Signal Jamming
		Pingblender /BlueSYN
		Battery Exhaustion
Malware	Intrusive or malicious software is installed on a device to interfere with activities, stealing data, or defraud a hostage target.	Skuller
		BlueBag
		CommWarrior
		Caribe
Fuzzer	Transforms data towards stack as well as the scheme and can identify bugs.	BlueStab/Bluetooth Stack Smasher
		Sonyericson Reset Display
		Nokia N70 L2CAP DoS
		L2CAP Header Overflow
		HCIDump Crash

RQ 4: Security issues that can become the cause of Bluetooth security unsatisfactory

This topic addresses issues with Bluetooth technology. Companies preparing security measures with Bluetooth technologies using the Bluetooth v5.0 standard will carefully consider the significance of protection. The flaw is connected to the encryption mechanism between two Bluetooth linking devices and has revealed flaws in how these devices exchange information about the minimum length of necessary keys and the keys themselves. Obviously, if you can reduce the length of keys without violating the pairing cycle, then an assault becomes much easier. Not all Bluetooth standards require a minimum duration of the encryption key, "the Security Notice states," it is conceivable that some manufacturers may have established Bluetooth devices where the size of the encryption key may use on EDR/BR link could be limited to a single octet by an attacking system. Where the key length can be reduced by an attacking device, the disclosure advises that the

attacking machine can then launch a brute force assault and have a better chance of successfully breaking the key and then being able to monitor or control traffic. And that's one big issue. Forget the speakers, headphones, and printers. The exchange of data and images between devices and vehicle systems, just to name but a few. It also remains unclear what data rates might be captured during the successful attack. There is no proof of effective exploitation of the weakness. But weakness is really a flaw, and as always, once it has been identified, the threats go up before improvements are implemented.

Table 4. Key Problems with Bluetooth Security

Sr. No	Year	Security Issues	Features	Analysis
Versions Before Bluetooth v1.2				
1	2003	Connection keys are unchanged and repeated for each combination, dependent on unit keys.	Fast connection. Upgraded SCO links Adaptive frequency hopping. Upgraded flow control and error detection. Upgraded flow specification. Upgraded synchronization capability.	A machine that uses unit keys will be using the same link key for each system it pairs to. That's a significant flaw in security key management.
2		The use of unit-based connection keys may contribute to spoofing and eavesdropping.		Once the unit key of a machine is revealed, any system with the key may spoof the device or any other device it has associated with. Furthermore, it may collect information on the connections of that system, whether they have been encrypted or not.
Versions Before Bluetooth v2.1				
3	2007	Devices using Security Mode 1 don't ever launch security mechanisms.	Encryption Resume and Pause Erroneous Data Reporting Extended Inquiry Response Link Timeout Supervision Event Changed Secure Simple Pairing Security Mode 4 Non-Flushable Packet Boundary Flag Sniff Subtracting	Systems that use Secure Mode 1 are essentially vulnerable. Secure Mode 3 (link-level security) is strongly recommended for v2.0 and earlier systems.
4		PINs could be too short.		Poor PINs can easily be guessed and are used to secure the generation of connection keys during pairing. Users tend to reach for fast PINs.
5		Control and complexity of PINs are lacking.		It may be difficult to establish the use of acceptable PINs in an organizational environment with a lot of users. Issues with scalability also cause security problems. The best alternative would be to produce the PIN using its random number generator for some of the devices getting paired.
6		Keystream encryption repeated after 23.3 hours of usage.		Keystream security relies on the Connection Key, Master BD ADDR, EN RAND, and Clock. Throughout a specific encrypted link, just the Master's clock will alter.
Bluetooth v3.0				
7	2009	The association model Just Works will not provide MITM security during pairing, resulting in an unauthenticated connection key.	AMP Manager Protocol (A2MP). Upgrades to L2CAP for AMP AMP Safety Changes. Upgrades to HCI for AMP.	For maximum security, systems must require MITM security during the SSP and refuse to acknowledge untrusted link keys that are produced using pairing Just Works.

8		SSP ECDH key combinations may be produced statically or otherwise loosely.		Poor ECDH key combinations reduce protection from SSP snooping, which can also encourage attackers to establish secret connection keys. All machines should be equipped with unique, strongly produced ECDH key pairs which regularly change.
9		The static SSP passkeys allow MITM attacks simpler.		During SSP, Passkeys provide protection for MITM. For every pairing, attempt devices should be using random, unique passkeys.
10		Security / Privacy Mode 4 systems (i.e., v2.1 and later) are enabled to return to any security mode when connected to devices that do not accept Protection Mode 4 (i.e., v2.0 or above).		The very worst-case scenario will be a system that falls back to Protection Mode 1, which does not provide security. In this scenario, NIST recommends that a Protection Mode 4 system return to Protection Mode 3.
Versions Before Bluetooth v4.0				
11	2009	The master key is using to encrypt broadcasts exchanged within all devices on the piconet.	802.11 Protocol Adaptation Layer Upgraded Power Control Unicast Without Connection HCI Write Order Key Length Encryption Standard AMP Check Methodology Reinforced USB, HCI, and SDIO transfer Corrected version for v 2.0 + EDR and v2.1 + EDR	Shared secret keys among more than the two parties encourage attacks by impersonation.
12		The cipher algorithm used in the Bluetooth BR / EDR authentication with E0 stream is extremely weak.		Through layering program-level FIPS-approved authentication over Bluetooth BR / EDR authentication, FIPS-approved authentication may be obtained.
13		Security may be violated by collecting the Bluetooth machine address (BD ADDR) and associating it with a specific user.		When the BD ADDR has been registered with a specific user, the behavior and position of that user could be monitored.
14		Authentication of devices is a clear challenge/reply to a common key.		Authentication of one-way issue/answer is subjected to a MITM attack. Bluetooth allows for shared authentication, which can be used to validate the authenticity of the devices
Bluetooth v4.0				
15	2010	Pairing LE does not provide protection for eavesdropping. Additionally, the pairing technique Just Works doesn't provide any MITM security.	Low Energy Errata for v2.0 + EDR, v2.1 + EDR, v3.0 + HS	If successful, the snoopers can catch transmitted secret keys during the LE pairing. Additionally, MITM attackers are able to catch and process data transferred between reliable devices.
16		LE Protection Mode 1 No protection measures are needed at level 1.		This is extremely secure, as with BR / EDR Protection Mode 1. Alternatively, LE Safety Mode 1 Stage 3 (authenticated matching or encryption) is strongly recommended.
Bluetooth v5.0				
17	2018	Allows for extremely low key length encryption	Speed twice, Support 2Mbps. Range 4x, compared to the old version. Low Power Requirement.	The Bluetooth BR / EDR standard up, including even version 5.1, requires a relatively short duration of the encryption key and does not

			Message Capacity 255 bytes. Better Security Control. Support for Iot Devices.	secure a hacker from disrupting the exchange of key lengths.
All Versions				
18		Connection keys could be improperly stored.		An attacker may access or change connection keys if they aren't safely stored and secured by access controls.
19		Pseudo-random number generator capabilities aren't understood.		The Random Number Generator (RNG) creates permanent or random numbers, which may decrease the protection mechanisms ' effectiveness. Bluetooth applications will utilize good NIST-based PRNGs.
20		The main Duration of Encryption is open for discussion.		The requirements v3.0 and earlier require the devices to discuss encryption keys as short as a bit. Bluetooth LE calls for a fixed key size of seven bytes. NIST recommends that both the BR / EDR (E0) and LE (AES-CCM) use the complete 128-bit main power.
21		There is no device verification.		The standard calls for only system authentication. Application-level protection may be implemented by the application creator via an overlay, including user authentication.
22		It does not provide end-to-end protection.		Only the separate connections are authenticated and encrypted. Data is decrypted in midpoints. End-to-end encryption can be given on top of the Bluetooth stack, utilizing extra security controls.
23		Security functions are often limited		The norm does not include verification, non-repudiation, and other resources. If required, the program developer may integrate certain resources in an overlay manner.

VI. DISCUSSION

This study is inspired by the rapid growth of Bluetooth use, which has created a large population of people who rely on Bluetooth devices for their everyday applications and activities, including computers, mobile phones, cars, headphones, printers, and many other types of equipment. Because of the large-scale use, it is important that academics recognize and analyze the Bluetooth system limitations. Security of information is crucial in all communication technologies, and Bluetooth technologies are no exception. The growing popularity of the use of wireless technology has brought new threats. Specified Bluetooth devices suffer from a number of security flaws that need to be properly understood to be resolved. Bluetooth systems are used to share a vast array of information, including audio, video, data, photos, and files. In doing so, they are massively enhancing our living standards and our daily lives.

Bluetooth is a technology that data to be shared in close proximity between compatible devices without needing to have a physical connection. Data sharing in electronic devices is rapidly growing. The digital identities and personal data for billions of users across the Web have been compromised in recent years by data breaches. Information technology is now an essential and fundamental part of industry and organization infrastructure. With the enormous growth and development of computer networks and the Internet, data traffic management and auditing are important to enhance the overall security and efficiency of a networked system. Bluetooth technology, disruptive agents can eavesdrop and compromise the integrity of communication as data is transmitted wirelessly. Intentionally, hackers can jam Bluetooth channels of communication, alter data, and even capture and retrieve confidential information. From the related work, the Bluetooth era of technology is upon us, and the devices are set to grow substantively. Whereas many security

hazards and technology-related threats remain, Scientists and engineers need to collaborate to examine these security risks. In literature review discusses the Bluetooth security literature topic to establish a comprehensive understanding of the prevalent aspects relating to Bluetooth pairing mechanisms in the field of security issues. Extensive work was carried out to classify the various problems that may occur in the Bluetooth technology, and innumerable attacks were reported. However, the ostentatious participation of prior research prompted the researchers to conduct additional research on Bluetooth technology-related security threats.

During the research methodology stage, a systematic approach would allow reviewers to generate a basic understanding of the topic. This research is focused on the security concerns of Bluetooth-embedded devices. In this study reading a number of articles on Bluetooth and its security risks, both academic and general. This section reviews for the systematic analysis were included. Systematic analysis phases include the identification and evaluation of study problems, the establishment of requirements, the quest plan, the hunt for repositories, the import of all findings into a library, and the exports to an excel spreadsheet, manual quest, data retrieval, and quality assurance.

This Next section would clearly describe the findings of the study and illustrate the research question. Bluetooth security strategies must evolve continuously to minimize emerging threats. Bluetooth signals can be intentionally interrupted or disrupted as any other wireless communication network. The unauthorized users can send incorrect or modified details to the computers. The first question is about the major possibilities threats of hacking and breaking the security of Bluetooth devices. We have shown that there are lots of potential technical attacks in which the Bluetooth security can breached. Bluetooth security threats can be classified into three main categories Disclosure threat, Denial of Service (DoS) threat, and Integrity threat. The next step illustrates further all possible Bluetooth attacks in detail that affect Bluetooth security. These possible attracts are listed: Man-In-The-Middle (MITM) Attack, MAC spoofing, Blue-smack attack, Blue bugging attack, “Blue-Snarfing” attack, “Blue-Printing” attack, DoS attack, BD_ADDR attack, SCO/eSCO attack, L2CAP guaranteed service attack, Fuzzing, Blue-Borne, Multi-Blue, “cabir worm” and “Helemoto”.

The second question was about identifying a Bluetooth device's threat classification and overview of prospective Bluetooth risks and their reasons to breach Bluetooth devices' security. This provided us insight into the motivation and understanding of the Bluetooth attacks which have to breach the Bluetooth device's security. The Bluetooth consists of nine separate Bluetooth-related threat classifications. Specific classifications of the attacks require different levels of threat. The Bluetooth discussion provides knowledge into the clarity of performing many of the listed Bluetooth Attacks. In the third question, we understand the Bluetooth threat taxonomy. We describe the threat level factor and their consequences on the security of Bluetooth devices when they are threatened from different possible attacks, which provided a set of requirements to improve the security of Bluetooth. The Bluetooth Threat Taxonomy (BTT) provides just a framework for classifying all threats based on Bluetooth. The classification of attacks can help determine the intensity of the threat, precautionary methods, and reactionary strategies. Understanding fundamental differences in threats of the same classification may help to apply prior knowledge to the new threats. Bluetooth Threat Taxonomy is made of nine separate classifications. Many of these categories are already common Cyber Security. The fourth question identifies security issues that may become unsatisfactory to the cause of Bluetooth safety. Based on such common security issues and risks found, more security problems are expected to be resolved.

V. CONCLUSION

Users are like to communicate in a secure medium. Bluetooth is a popular and effective wireless platform for data exchange. The Bluetooth devices growth is increasing, and the pattern is expected to continue; there is a need to resolve the growing security conceptions of Bluetooth technology. This study addressed the possible attacks of Bluetooth technology. We have shown that there are many possible attacks in which Bluetooth security can be compromised. These threats can be grouped into three main categories, Disclosure threat, Denial of Service (DoS) threat, and Integrity threat. In this study, we provided a comprehensive study of the Bluetooth technology security flaws. Users are not well known for such security risks. Furthermore, some of the threats to Bluetooth technology go unnoticed or unreported. A major advantage for hackers would be the lack of knowledge for Bluetooth attacks. Users can remain safe with a bit of knowledge about these threats. Bluetooth is a revolutionary and inspiring technology that reinvigorates the way we communicate. Nevertheless, the current security protocols in Bluetooth aren't enough. Bluetooth, therefore, is vulnerable to a number of threats. This study work will help researchers explore new forms of attacks that are still immaterial through the information of these current threats and further examination, as well as potential deception combinations. The Bluetooth technology research and development departments can focus on these threats and improve better built-in security precautions for their technology. Finally, this study will encourage Bluetooth manufacturers to come up with a minimum level of safety measures to ensure the integrity of their devices.

ACKNOWLEDGMENT

We are especially thankful to our respected supervisor and course instructors [Dr. Kashif Bilal (Assistant professor Comsats University Islamabad, Pakistan) & Dr. Muhammad Farhan (Assistant professor Comsats University Islamabad, Sahiwal, Punjab Pakistan)] who provided valuable expertise that greatly assisted the research, although they provided us more precious guidelines and valuable suggestions to moderate this paper and in that line improved the manuscript significantly.

REFERENCES

[1] Xu, F., Diao, W., Li, Z., Chen, J. and Zhang, K., BadBluetooth: Breaking Android Security Mechanisms via Malicious Bluetooth Peripherals. In NDSS., (2019).

[2] How Bluetooth works. Retrieved from http://en.kioskea.net/contents/bluetooth/bluetooth-fonctionnement.php3.

[3] Lee, C. S. Bluetooth security protocol analysis and improvements., (M.Sc. thesis). San Jose State University. Retrieved from http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf., (2006).

[4] Larson, S., Every single Yahoo account was hacked-3 billion in all. CNN Tech, October, 4., (2017).

[5] Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., Markov, Y., Comanescu, O., Eranti, V., Moscicki, A. and Margolis, D., Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (2017) (1421-1434). ACM.

[6] Rhodes, C. Bluetooth security. (East Carolina University, (2006) 6-9.

[7] Padgette, J., Scarfone, K. and Chen, L., Guide to Bluetooth security. NIST Special Publication, 800(121) (2012) 25.

[8] Dell, P. and Ghori, K.S.U.H. A simple way to improve the security of Bluetooth devices. In 2008 International Symposium on Applications and the Internet (2008) (444-447). IEEE.

[9] AL BAHAR, M., Dissertations in Forestry and Natural Sciences.

[10] Browning, D. and Kessler, G.C., Bluetooth hacking: A case study., (2009).

[11] Hodjat, A. and Verbauwhede, I., The energy cost of secrets in ad-hoc networks (short paper). In Proc. IEEE Circuits and Systems Workshop (CAS).,(2002).

[12] Candolin, C., Security issues for wearable computing and Bluetooth technology. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, Finland., (2000).

[13] Laurie, B. and Laurie, A., Serious flaws in Bluetooth security lead to the disclosure of personal data. AL Digital Ltd. Technical report. http://bluestumbler. Org., (2003).

[14] Jakobsson, M. and Wetzel, S., Security weaknesses in Bluetooth. In Cryptographers' Track at the RSA Conference (2001) (176-191). Springer, Berlin, Heidelberg.

[15] Gehrmann, C. and Nyberg, K., November. Enhancements to Bluetooth baseband security. , (2001) In Proceedings of Nordsec 191-230).

[16] Kügler, D., 2003, January., Man in the Middle., Attacks on Bluetooth. In International Conference on Financial Cryptography (149-161). Springer, Berlin, Heidelberg.

[17] Singelée, D. and Preneel, B., 2004. Security overview of Bluetooth. COSIC Internal Report, (2004).

[18] Karygiannis, T. and Owens, L., 2002. Wireless network security. NIST special publication, 800 (2004) 48.

[19] Aissi, S., Gehrmann, C. and Nyberg, K.,. Proposal for enhancing Bluetooth security using an improved pairing mechanism. In Bluetooth architecture review board at the Bluetooth all-hands meeting., (2004).

[20] Sayegh, A.A. and El-Hadidi, M.T., September. A modified secure remote password (SRP) protocol for key initialization and exchange in Bluetooth systems. In First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05) (2005) (261-269). IEEE.

[21] Giousouf, A. and Lemke, K., Bluetooth Security. Communication Security Department Ruhr University, Bochum.

[22] Shaked, Y. and Wool, A., 2005, June. Cracking the Bluetooth pin. In Proceedings of the 3rd international conference on Mobile systems, applications, and services (2005) (39-50).

[23] Lindell, A.Y., 2008. Attacks on the pairing protocol of Bluetooth v2. 1. Black Hat USA, Las Vegas, Nevada.

[24] Barnickel, J., Wang, J. and Meyer, U., 2012, June. Implementing an attack on Bluetooth 2.1+ secure, simple pairing in passkey entry mode. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications ,(2012) (17-24). IEEE.

[25] Haataja, K. and Toivanen, P., 2010. Two practical man-in-the-middle attacks on Bluetooth secure, simple pairing and countermeasures. IEEE Transactions on Wireless Communications, 9(1) (2010) 384-392.

[26] Chang, R. and Shmatikov, V., Formal analysis of authentication in Bluetooth device pairing. FCS-ARSPA07(2007) 45.

[27] Das, A.K., Pathak, P.H., Chuah, C.N. and Mohapatra, P., 2016, February. Uncovering privacy leakage in ble network traffic of wearable fitness trackers. In Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications., (2016) (99-104).

[28] Levi, A., Çetintaş, E., Aydos, M., Koç, Ç.K. and Çağlayan, M.U., 2004, October. Relay attacks on Bluetooth authentication and solutions. In International Symposium on Computer and Information Sciences (278-288). Springer, Berlin, Heidelberg.

[29] Aissi, S., Gehrmann, C. and Nyberg, K.,. Proposal for enhancing Bluetooth security using an improved pairing mechanism. In Bluetooth architecture review board at the Bluetooth all-hands meeting., (2004).

[30] Ryan, M., 2013. How Smart is Bluetooth Smart? SchmooCon 9.

[31] Mutchukota, T.R., Panigrahy, S.K. and Jena, S.K., 2011, August. Man-in-the-middle attack and its countermeasure in Bluetooth secure, simple pairing. In International Conference on Information Processing (367-376). Springer, Berlin, Heidelberg.,

[32] Scarfone, K. and Padgette, J., 2008. Guide to Bluetooth security. NIST Special Publication, 800(2008M).121.

[33] Minar, N.B.N.I. and Tarique, M., Bluetooth security threats and solutions: a survey. International Journal of Distributed and Parallel Systems, 3(1) (2012) 127.

[34] Sandhya, S. and Devi, K.S., 2012, November. Contention for man-in-the-middle attacks in Bluetooth networks. In 2012 Fourth International Conference on Computational Intelligence and Communication Networks (2012) (700-703). IEEE.

[35] Lonzetta, A.M., Cope, P., Campbell, J., Mohd, B.J. and Hayajneh, T., Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3) (2018) 28.

[36] Browning, D. and Kessler, G.C., Bluetooth hacking: A case study., (2009).

[37] Dhuri, S., Bluetooth Attack and Security. Int. J. Curr. Trends Eng. Res, 3(2017) 76-81.

[38] Hassan, S.S., Bibon, S.D., Hossain, M.S. and Atiquzzaman, M., Security threats in Bluetooth technology. Computers & Security, 74 (2018) 308-322.

[39] Satam, P., Satam, S. and Hariri, S., Bluetooth Intrusion Detection System (BIDS). In 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA) (2018) (1-7). IEEE.

[40] Dubey, V., Vaishali, K., Behar, N. and Vishwavidyalaya, G., A Review on Bluetooth Security Vulnerabilities and a Proposed Prototype Model for Enhancing Security against MITM Attack. Int. J. Res. Stud. Comput. Sci. Eng, (2015) 69-75.

[41] Tsira, V. and Nandi, G., 2014. Bluetooth technology: Security issues and its prevention. Int. J. Comput. Appl. Technol, 5(2014) 1833-1837.

[42] Zeadally, S., Siddiqui, F. and Baig, Z., 25 Years of Bluetooth Technology. Future Internet, 11(9) (2019) 194.

[43] Dunning, J., Taming the blue beast: A survey of Bluetooth based threats. IEEE Security & Privacy, 8(2)(2010) 20-27.

[44] Gostev, A. and Maslennikov, D., Mobile malware evolution: An overview. Kaspersky Labs Report on Mobile Viruses., (2006).

[45] Colleen, R., Bluetooth security. East Carolina University., (2006).

[46] Surendiran,R., and Alagarsamy,K., 2012. "An Extensive Survey on Mobile Security and Issues". SSRG International Journal of Computer & organization Trends (IJCOT), 2(1), pp.39-46.

[47] Hassan, S.S., Bibon, S.D., Hossain, M.S. and Atiquzzaman, M., 2018. Security threats in Bluetooth technology. Computers & Security, 74 (2018) 308-322.