Bluetooth Connect: Messaging App for Offline Communication Over Wide Range Using Mesh Networking or Range Extenders

Abeye Tewodros Tilahun[1], Ananya Samuel Adane[2], Dawit Hadush Abrha[3], Ebenezer Mulugeta Woldehana[4], Nawid Barakzai[5], Dr. Sonal Sharma[6]
[1,2,3,4,5]*UG Student, Dept. Of CSE, Jain University, Bangalore, India*
[6]*Associate Professor, Jain University, Bangalore, India*

***Abstract*—When Internet service is not available, communication might be difficult. An Internet crash can arise due to natural catastrophes like earthquakes, floods, tornadoes, and disasters created by humans, like cyber attacks, censorship, police or security service actions, or system malfunctions. Especially in the event of a tragedy, people who live in these situations frequently find it challenging to communicate with one another and request help. An Android point-to-point chat tool using Bluetooth is designed and implemented in this article. Users can communicate directly with one another using our technology. The software enables Bluetooth text messaging connections between users. Two mobile devices connected by a Bluetooth Socket can interact without the Internet. We use Google Firebase for authentication in this Android-based app.**

Keywords—Internet, Bluetooth, Wireless, Network, Communication

I. INTRODUCTION

Information transmission between two points without the use of wires, cables, or any other physical medium is referred to as wireless communication. A variety of technologies, including radio waves, satellites, and infrared, can be used for wireless communication. Over time, wireless communication has quickly developed to take the place of the intricate conventional telephone system [1].

A. The Gap We Saw

One of the most significant innovations of our time, the Internet, has gained popularity and spread swiftly across the globe, but the cost of Internet connectivity is frequently exorbitant in developing nations; according to the United Nations, nearly three-quarters of people in the 46 least-developed countries have never been online, and almost 3 billion people—or 37% of the global population—have never used the Internet. As described by the UN International Telecommunication Union (ITU), 96% of the 2.9 billion individuals who have not used the internet reside in developing nations [2]. For example, mobile users in India may have reached 1.16 billion, but of the 5.97 lakh villages in India, over 25,000 villages still do not have mobile or Internet connectivity [3].
Further, where internet access is available, some regions frequently experience outages due to a variety of factors, including system failures, censorship, cyber attacks, and natural disasters like earthquakes, floods, and tornadoes, as well as human-caused disasters like cyber attacks, censorship, and police or security service actions. Network towers, cables, and other internet infrastructure would be damaged in such crisis conditions, putting the area in danger and preventing residents from communicating with one another in an emergency. Having a backup communication method is essential [4].
This need may be met by Bluetooth, wireless technology frequently used in mobile devices, which offers a way for long-distance offline communication.

B. Bluetooth Technology Overview

Bluetooth technology is a wireless communication technology that allows devices to communicate with each other over short distances without the need for wires or cables. It was developed by Ericsson in 1994 and is named after Harald Bluetooth, a Danish king from the 10th century who was known for his ability to unite different groups of people.
Bluetooth technology uses radio waves to transmit

data between devices. The radio waves used by Bluetooth are in the 2.4 GHz frequency range, which is an unlicensed frequency band that is available for use by anyone. The maximum range of Bluetooth is typically around 10 meters (33 feet), although this can be extended with the use of Bluetooth repeaters or other devices.

One of the main advantages of Bluetooth technology is its ease of use. Devices can be paired with each other simply by placing them close together and following a few simple steps. Once paired, devices can communicate with each other without the need for any additional setup or configuration.

Bluetooth technology is used in various applications, including wireless headphones, speakers, keyboards, mice, and game controllers. It is also used in the automotive industry for hands-free calling and audio streaming, as well as in healthcare for wireless medical devices.

There are several different versions of Bluetooth technology, each with its features and capabilities. The most recent version is Bluetooth 5.2, which was released in 2020. Some of the features of Bluetooth 5.2 include improved data transfer speeds, increased range, and improved security features.

In addition to the standard Bluetooth protocol, several other protocols are based on Bluetooth technology. These include Bluetooth Low Energy (BLE), which is designed for low-power devices such as fitness trackers and smartwatches, and Bluetooth Mesh, which is designed for large-scale networks of devices such as smart lighting systems.

Bluetooth establishes a secure connection between two devices by exchanging PINs or personal identification numbers. This is referred to as "pairing." The master and slave pairing method in Bluetooth communication allows two devices to be connected. One device (the master) initiates the connection, while the other (the slave) reacts and follows the master's orders. This pairing process is widely used to enable smooth communication between Bluetooth devices such as wireless headphones, speakers, and keyboards. To guarantee communication privacy and security, the devices exchange a unique pairing code during the operation, which only approved devices can use to connect. Master's device can communicate with up to seven slave devices to establish a piconet network. Two or more piconets combined form a scatternet, which can be used to overcome Bluetooth range limitations. A scatternet is created when devices act as master' or slave' devices in many piconets at the same time.

Potential security threats associated with Bluetooth include eavesdropping, data interception, and malware attacks. Bluetooth security has evolved over the years and the latest versions of Bluetooth have introduced stronger security measures to address these threats. Bluetooth devices can be secured by keeping devices updated with the latest firmware and avoiding public Wi-Fi networks when using Bluetooth [5].

Overall, Bluetooth technology has become an essential part of modern life, enabling wireless communication between devices in a variety of applications. As technology continues to evolve, Bluetooth will likely continue to play an important role in connecting devices and enabling new types of applications.

C. Our Mission

In this paper, Bluetooth Connect is introduced. Users of this messaging app can communicate over longer distances than those covered by conventional Bluetooth connections thanks to mesh networking and range extenders. We go over the application's architecture and implementation, as well as its capabilities for file sharing, offline message queuing, and group messaging. We also examine the performance of Bluetooth Connect in several trials, comparing its range and dependability to standard Bluetooth connections. Our findings show that Bluetooth Connect is an effective method for offline communication across a large region and has the potential to offer a valuable platform for collaboration in places without access to the internet.

II. LITERATURE SURVEY

Numerous studies on using Bluetooth technology for short-distance communication are being conducted. This literature review is carried out to comprehend how Bluetooth technology works, how it may be utilized in short-distance communication, what approaches can be employed to secure Bluetooth communication and to evaluate previously completed Bluetooth-based messaging apps.

Even Though Bluetooth cannot completely replace the Internet for the broad public, it can be a superior solution for a specific target. A 2005 paper, outlined the differences between the Internet and Bluetooth

technology. The comparison in terms of capacity, network topology, security, QoS support, and power consumption. Some of these properties, such as data link types and performance, topologies, and medium access control, are stable and clearly defined by standards. Others, such as power consumption, QoS, and security, are open challenges where technology is always evolving in terms of both standards and implementations. As a result, an efficient solution to the hidden terminal problem was discovered, as was the support for real-time transmissions in such a way that real-time traffic constraints map the user QoS requirements, the development of efficient routing algorithms in mobile multihop environments, increasing data transfer security while maintaining ease of use, mitigating interference, and the use of new multiplexing techniques such as UWB and MIMO [6].

The construction of an Android chatting software that communicates using Bluetooth connectivity is described in the paper "Bluetooth Chatting: An Android Chatting app based on Bluetooth Connectivity." Together with a detailed explanation of the app's design and components, there is also a step-by-step user manual. The app's performance is assessed in terms of speed, dependability, and user-friendliness, and a comparison with other apps available on the market is given. Instant messaging is now often done via apps like WhatsApp, Telegram, WeChat, Hangouts, and others. However, these apps rely on the Internet, i.e., either cell data, which can be a paid carrier, or Wi-Fi, which isn't always available and, when it is, varies in connection strength from location to location. The Android mobile network chat module includes a smartphone feature called Bluetooth that is integrated into the platform. A Bluetooth-enabled chat system can be built using the Android platform using the extensive set of Bluetooth APIs that are included with the Android device. Bluetooth is a Wi-Fi substitute for sending data over short distances. Half-duplex transmission rates of up to 721 kilo-bits per second (Kbps) in one direction and 57.6 Kbps in the other are possible when using it in networks or communications. The Bluetooth module separates Android phones into client and server roles, enabling real-time conversation between friends and strangers. To serve as a server when two devices are connected, one of them must keep a BluetoothServerSocket open. The server socket's function is to monitor incoming connection requests and, in response to a successful request, to send a Bluetooth socket. Getting a Bluetooth device object is necessary before you can connect to a remote device. Developers can create end-to-end encrypted communications utilizing public/private key science with the help of Virgil Security's Android SDK. Before a user's device sends a message, it is encrypted, and only the intended recipient (the end-user) may decrypt it. [7].

El-Seoud and Taj-Eddin (2016) developed an Android mobile Bluetooth chat messenger as a collaborative and interactive learning tool. To improve communication between students and teachers in learning environments, the messaging application's design and implementation are described in detail in this paper. With capabilities including group chat, file sharing, and message archiving, the application connects devices using Bluetooth. The application proved effective in encouraging collaborative learning and enhancing communication between students and teachers, according to a user survey the authors did to evaluate it. They conclude that the program could improve learning and foster better collaboration and communication in the classroom [8].

Pirani et al. (2018) researched Bluetooth and Wi-Fi text messaging systems. The writers discuss various messaging protocols that can be employed as well as the benefits and drawbacks of such technologies for messaging. Also, they examine several Bluetooth or Wi- Fi-based messaging systems that are already in use, including both for-profit and free options. While Bluetooth messaging has the benefit of functioning in locations without Wi-Fi or cellular coverage, the authors point out that it has a constrained range and might be interfered with. On the other hand, Wi-Fi messaging offers a wider range and more rapid data transfer rates but necessitates a Wi-Fi network. The choice between the two technologies, according to the authors, relies on the requirements of the individual applications. Both technologies have advantages and disadvantages [9].

Deb and Sinha (2014) developed an Android mobile application that employs Bluetooth technology called Bluetooth Messenger. The program, which aims to offer a substitute for conventional messaging apps that require internet connectivity, is described in detail in the article with its design and implementation. The

program's functions include file sharing, group messaging, and archiving. According to the user research, the authors conducted to test the application, the app provided a reliable means for communicating over short distances. The authors concluded that the program has the potential to serve as a valuable means of interaction in locations with poor or no internet access, such as rural or isolated areas [10]

The paper "Bluetooth Message Hopping Chat Application" set out to create network transparency and enable secure device communication as its main objective. It aimed to transfer messages beyond Bluetooth's standard range of 10 m via intermediate devices, which act as bridges connecting two devices outside the Bluetooth range. The message content, the recipient's MAC address, and the sender's MAC address are all included in the message transmission. If the sender does not get an acknowledgment message from the recipient for a predetermined amount of time, the proposed system additionally incorporates a system to generate delivery failures.

Multi-point relay flooding was used to avoid the blind sending of messages. The Multi-Point Relay technique broadcasts the messages to only those nodes likely to be on the destination route until the destination is found. The paper tries to address security by generating a public-private key using the RSA (Rivest–Shamir–Adleman) algorithm. The main disadvantage is that the app must be running at all times, and the Bluetooth of the intermediary devices must be turned on even when they are not delivering messages, causing battery consumption to rise. The paper concludes that Bluetooth messaging is a feasible alternative that overcomes low internet connectivity or battery power consumption problems, and it suggests that the security of the app needs to be improved since it handles very sensitive personal information [11].

Bluetooth device range can be expanded by upgrading to a newer device with improved Bluetooth technology, such as Bluetooth 4.0 or 5.0 or the newest 5.2 and 5.3 versions, which not only provide faster connectivity but also cover a larger area. Another option is a Bluetooth range extender, which acts as a signal booster or repeater. The extension allows you to connect devices up to 150 feet apart outside and up to 70 feet apart indoors. If you require a longer range, connect two range extenders in a daisy chain configuration to extend the range beyond the initial 150-foot limit. It's worth noting that Bluetooth 4.0 includes more security features than previous versions, making it a more secure option [12].

According to the patent paper "Apparatus and methods for extending Bluetooth device range," A few meters to a few tens of meters is the operating range of the Bluetooth wireless communication protocol, making it a relatively short-range technology. Unfortunately, the limited range of the majority of Bluetooth devices prevents them from being useful in a wide range of situations. We carefully reviewed previous examples of radio frequency (RF) amplifiers used in range extender devices. They re-transmit radio energy received inside the Bluetooth ISM frequency range at greater power and frequency. The research proposed a "smarter" technique of increasing range by employing equipment that could differentiate between "actual" Bluetooth signals and noise, re-transmitting only the genuine signals. On the other hand, for these radio frequency amplifiers, simply to improve the radio frequency (RF) signal, one must take into account interference from other ISM-band devices as well as Bluetooth transmit (Tx) power control, which can be utilized between Bluetooth devices to carefully regulate the energy received at the antenna for the best reception. Therefore, we concluded that it is advised to increase a Bluetooth app's range while utilizing conventional Bluetooth communication methods and continuing to be compatible with Bluetooth communication standards. Using at least two Bluetooth communication profiles, a Bluetooth range extender device is one illustration of a gadget for increasing the range of Bluetooth devices, with the Bluetooth range extender device implementing both the first function for a first standard Bluetooth communication device and the second role for a second standard Bluetooth communication device [13].

A security examination of the Bridgefy mesh messaging app, used in situations where internet connectivity is poor or absent, is presented in the paper "Mesh Messaging in Large-Scale Protests: Cracking Bridgefy." The authors found several flaws in the app's protocol that an attacker could use to

intercept, alter, and inject messages. The study emphasizes the significance of security in mesh networking-dependent communication apps and the demand for thorough testing and validation before deployment in sensitive scenarios. Despite using an older version of the app, the study sheds important light on the security concerns related to mesh messaging apps and the necessity of ongoing security testing and monitoring [14].

A device-to-device (D2D) routing protocol for self-organized mobile phone mesh networks is provided in the article "Bluetooth-based device-to-device routing protocol for self-organized mobile phone mesh network" by Fan et al. To enable mobile phones to forward data packets to other phones in the network, the authors suggest a multi-hop routing system. The protocol's design is discussed in detail, and the article rates the protocol's efficiency in terms of packet delivery rate, end-to-end delay, and overhead. The outcomes show that the suggested protocol allows a low end-to-end delay and a high packet delivery ratio with little overhead. The paper offers helpful insights for researchers and practitioners attempting to create device-to-device communication protocols for mobile phone mesh networks [15].

In their work published in 2018, Sun, Mu, and Susilo look into man-in-the-middle attacks against the Secure Simple Pairing (SSP) security feature found in the Bluetooth v5.0 standard. The authors point out holes in the SSP protocol that let an attacker intercept and interfere with pairing two Bluetooth devices, giving them access to private information and services. They suggest a defense known as Simple Concurrent Authentication Protocol (SCAP), which increases pairing process security using a concurrent authentication approach. Using simulation and analysis, the authors assess SCAP's performance and effectiveness and demonstrate that it offers a significant increase in security over the SSP protocol that is currently in use. They concluded that the suggested countermeasure is an effective way to solve the security flaws in the Bluetooth v5.0 standard [16].

The study by Albahar et al., titled "New Hybrid Encryption Algorithm Based on AES, RSA, and Twofish for Bluetooth Encryption," presents a unique hybrid encryption algorithm for Bluetooth encryption based on the Rivest-Shamir-Adleman (RSA), Twofish, and Advanced Encryption Standard (AES) algorithms. Because Bluetooth communication has a short range and is susceptible to interference, the authors combine these techniques to increase its security. The suggested algorithm's design and implementation are presented in this work, together with an assessment of the algorithm's efficiency in terms of decryption and encryption times, key size, and security. The outcomes show that the suggested algorithm while retaining reasonable decryption and encryption times offers improved security in comparison to existing encryption algorithms. Practitioners and researchers interested in strengthening Bluetooth communication security will find the study to be a valuable resource [17].

An overview of Bluetooth security problems and solutions is provided in the paper "Bluetooth Security Threats and Solutions: A Survey" by Minar. The paper addresses Bluetooth technology's weaknesses, including eavesdropping, man-in-the-middle attacks, denial-of- service assaults, and unauthorized access, and analyses the security measures now in place to deal with these problems. The paper investigates the authentication, encryption, and authorization security elements of Bluetooth protocols and highlights their shortcomings. The author also reviews previous research on Bluetooth security and discusses suggested fixes to reduce security risks. The paper's conclusion makes recommendations for future study areas to strengthen Bluetooth technology security. For practitioners and researchers interested in Bluetooth security, the paper offers a thorough assessment of Bluetooth security challenges and solutions [18].

III. DISCUSSION

Understanding the application of Bluetooth technology for communication was the goal of this study of the literature. The review examined Bluetooth technology's operation, its application in communication, Bluetooth communication security measures, and previously created Bluetooth-based messaging apps.

Using half duplex transmission speeds of up to 721 Kbps, the review discovered that Bluetooth can be used as an alternative to Wi-Fi for data transmission over distances. The Android platform and its APIs can be used to create Bluetooth-based messaging systems with end-to-end encryption made feasible by the use of public-private key encryption. Using multi-point

relay floods and public-private key encryption using the RSA technique, the article "Bluetooth Message Hopping Chat Application" sought to provide a safe and open device communication system. But because the app must always be active, battery usage increases.

A disadvantage of Bluetooth devices is their short range, and past attempts to increase that range by using radio frequency amplifiers have been constrained by interference from other devices and power control restrictions among Bluetooth devices, according to the review. The conclusion implies that it could be wise to extend the range of Bluetooth devices using established techniques and Bluetooth communication standards compatibility.

According to the evaluation of the research, Bluetooth technology can be a practical substitute for communication, and the Android operating system's APIs make it possible to integrate it into messaging apps. While maintaining Bluetooth communication standards, the range of Bluetooth devices can be increased. Since these apps deal with sensitive user data, their security might need some work.

Figures

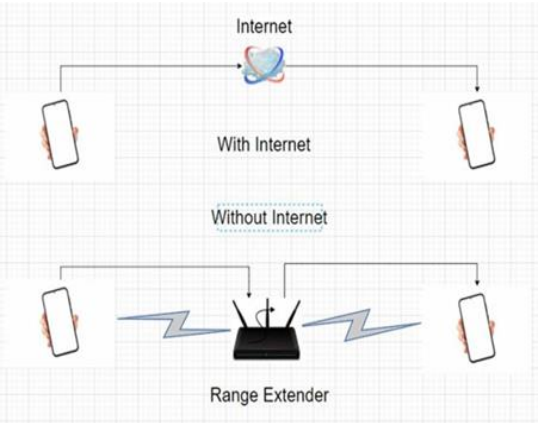

Fig.1. Conceptual Block Diagram

Fig. 1 illustrates how a link between two users functions in the absence of the internet or phone towers. The two gadgets can be connected in two different ways. One makes use of mesh networking, while the other uses Bluetooth range extenders.

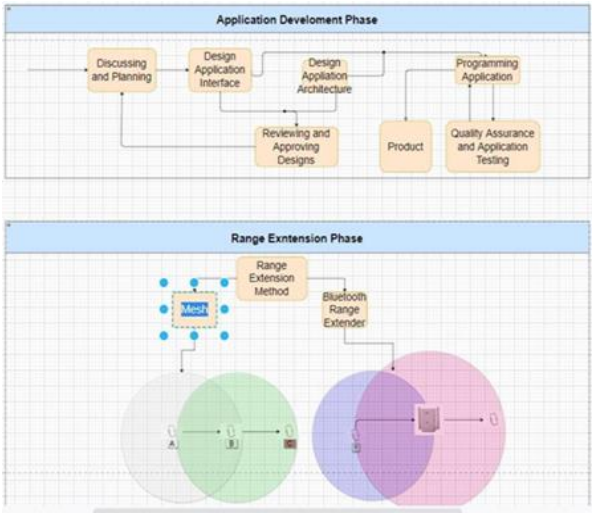

Fig.2. The operational flow of the work

The Bluetooth Range Extender is a tool that can increase a device's range so that other users can access it and establish connections. Two devices, for instance, are outside of range as shown in the diagram. Therefore, the device can increase the range and connect by using a Bluetooth Range Extender.

According to the mesh concept, devices can send data to their target addresses by using other devices as a conduit. For instance, suppose there are three users at points A, B, and C (Fig. 2). Data is being sent from Point A to Point C. They are further apart, though. Both users can reach Point B. The shared data will initially travel to point B using the mesh principle and then it is redirected to point C.

IV.METHODOLOGY

A. Testing Previous Works

Over the years, developers have made attempts to develop a similar solution. They have developed software that doesn't need Internet access to operate. Bluetooth technology is used by these applications to link the host device to other devices. Additionally, they are designed to provide a certain function, such as sending texts or sharing files, etc. Our project's primary objective was to combine these functionalities into a single application. It is a comprehensive messaging tool that users may use to share files, make video chats, and communicate via texts and photographs.

B. Researching

To close the gaps in our project, a study was carried out. Security concerns have been the main ones thus

far. The fact that Bluetooth technology is highly vulnerable to attacks is one of its drawbacks. Since users place a high value on security, numerous studies have been done to determine the best procedures, formulas, and strategies for enhancing the security of our application. Users will feel more secure knowing that their data is safe because of this.

C. Proposing our idea to reviewers

The main idea of the project was frequently presented while it was being worked on. Later, several suggestions about how to enhance our project were gathered. These reviews also included feature enhancement recommendations, which were helpful to us in our quest.

D. Advice from Our Mentors

A seasoned Android developer has been hired to serve as a mentor for our project. The mentor has provided our team with advice and assistance throughout the project to ensure its success. He has reviewed, commented, and offered suggestions for improvement.

E. Taking Courses

People with various levels of technical experience make up our team. We had to enroll in classes and explore a variety of study materials for us to be on the same page.

V.CONCLUSION

While the Internet performs a vital and seemingly faultless function, we frequently forget that some people reside in areas with minimal or no Internet connectivity. This essay suggested a better answer by reviewing the ways proposed to address the problem. Bluetooth is helpful in this situation because it has lower costs and battery consumption when compared to other kinds of media such as the internet and Wi-Fi hotspots. As a result, developing a system that is not dependent on the Internet is perfect. As a result, a Bluetooth-enabled application was created and deployed using the Android Framework and a variety of different programming languages.

The application is divided into four main sections: searching, authentication, matching, and file sharing. The searching system operates by scanning and finding devices within its range and preparing them for pairing through a key, such as a numeric code or encrypted data link before data exchange begins. Authentication can be accomplished by the use of a password or through public key authentication, which generates a key pair with a public and private key from a single device. Before the devices are linked and ready for use, the users' identities will be validated. As a result, there will be no uncertainty about the security of Bluetooth technology, and it will become a more secure communication method. The devices that are linked can then share files and other stuff.

One of Bluetooth's restrictions is that it only works within a specific range. However, after extensive investigation, solutions to enhance the range have been discovered. This could be accomplished through the use of mesh networking or a Bluetooth extender device. Mesh networking is a system in which, when one device's range is limited and it cannot reach the other device for data exchange, a third device functions as a bridge between the two. For the mesh to function, this third device must be within range of both devices. Because the data is encrypted, it is passed through an intermediary or third device without being accessed. The Bluetooth extender, on the other hand, works by boosting the range so that it can connect with the other device for data transmission.

Due to its growth, wireless communication will eventually surpass conventional networks. In the future years, it is anticipated that mobile and wireless devices will account for two-thirds of all IP traffic. There will be 20.4 billion Internet of Things (IoT) devices online in that same year [19]. The future of the internet is believed to be represented by this technology.

REFERENCES

[1] S. S. Chauhan, “What is Wireless Communication? | Introduction, History, Types, and Services - Mahalpur,” Mahalpur, Sep. 20, 2022. https://mahalpur.com/what-is- wireless-communication-introduction-history-types-and-services/

[2] S. Reporter, “More than a third of world’s population have never used internet, says UN,” The Guardian, Oct. 19, 2022.

[3] https://www.theguardian.com/technology/2021/nov/30/mo re-than-a-third-of-worlds-population-has-never-used-the- internet-says-un

[4] R. Shrivastava, “Over 25000 villages in India still lack internet connectivity, Lok Sabha told,” India Today, Mar. 18, 2021.

[5] https://www.indiatoday.in/technology/news/story/

over- 25000-villages-in-india-still-lack-internet-connectivity-lok- sabha-told-1780758-2021-03-18

[6] P. Vavra, "Why is Rural Internet So Bad? - BLiNQ Networks," BLiNQ Networks, Jul. 13, 2020. https://blinqnetworks.com/why-is-rural-internet-so-bad/

[7] T. Marks, "How Secure is Bluetooth? A Full Guide to Bluetooth Safety," VPNOverview.com, Feb. 06, 2023. https:// vpnoverview.com/privacy/devices/bluetooth/

[8] Ferro and F. Potortì, "Bluetooth and wi-fi wireless protocols: a survey and a comparison," IEEE Wireless Communications, vol. 12, no. 1, pp. 12–26, Feb. 2005, doi: 10.1109/ mwc.2005.1404569.

[9] H. Satnami, D. Kumar, and S. Wadhwa, "Bluetooth Chatting: An Android Chatting app based on Bluetooth Connectivity," International Journal of Engineering Development and Research, vol. Volume 11, no. Issue 1, Art. no. IJEDR2102035, Jun.2021,[Online].Available: https://www. ijedr. org/papers/IJEDR2102035.pdf

[10] M. S. A. El-Seoud and I. a. T. F. Taj-Eddin, "Developing an Android Mobile Bluetooth Chat Messenger as an Interactive and Collaborative Learning Aid," Advances in Intelligent Systems and Computing, pp. 3–15, Sep. 2016, doi: 10.1007/978-3-319-50340-0_1.

[11] Z. Pirani, B. Zaveri, R. Shaikh, and E. Shaikh, "Survey of Text Messaging System using Bluetooth and Wi-Fi," International Journal of Computer Applications, Feb. 2018, doi: 10.5120/ijca2018916504.

[12] A.Deb and S. Sinha, "Bluetooth Messenger: an Android Messenger app based on Bluetooth Connectivity," IOSR Journal of Computer Engineering, vol. 16, no. 3, pp. 61–66, Jan. 2014, doi: 10.9790/0661-16336166.

[13] Govind, T. Shaikh, K. Karande, I. Shaikh, and H. Vaghela, "Bluetooth Message Hopping Chat Application," International Journal of Computer Techniques, vol. Volume 2, no. Issue 5, Art. no. 2394–2231, Oct. 2015, [Online]. Available: http://www.ijctjournal.org/Volume2/Issue5/IJCT-V2I5P19.pdf

[14] K. C. Mba, "How To Increase Bluetooth Range - The Gadget Buyer | Tech Advice," The Gadget Buyer | Tech Advice, Mar. 02, 2023. https://thegadgetbuyer.com/how-to-increase-bluetooth-rang/

[15] B. F. Miller, "Apparatus and Method for Extending Bluetooth Device Range," US8983384B2, Mar. 17, 2015 [Online]. Available:https://patents.google.com/patent/US8983384B2/en

[16] M. Albrecht, J. Blasco, R. K. Jensen, and L. Mareková, "Mesh Messaging in Large-Scale Protests: Breaking Bridgefy," Lecture Notes in Computer Science, pp. 375–398, May 2021, doi: 10.1007/978-3-030-75539-3_16.

[17] A.-H. Fan, Z. Tang, W. Wu, Y. Tang, and D. Lin, "Bluetooth- based device-to-device routing protocol for self-organized mobile-phone mesh network," Eurasip Journal on Wireless Communications and Networking, vol. 2020, no. 1, Dec.2020, doi: 10.1186/s13638-020-01768-4.

[18] Sun, Y. Mu, and W. Susilo, "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure," Personal and Ubiquitous Computing, vol.22, no.1, pp. 55 –67, Feb.2018, doi:10.1007/s00779-017-1081-6.

[19] M. A. Albahar, O. Olawumi, K. Haataja, and P. Toivanen, "Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption," Journal of Information Security, vol. 09, no. 02, pp. 168–176, Apr. 2018, doi: 10.4236/jis.2018.92012.

[20] N. B.-N. I. Minar, "Bluetooth Security Threats And Solutions: A Survey," International Journal of Distributed and Parallel Systems, vol. 3, no. 1, pp. 127–148, Jan. 2012, doi: 10.5121/ ijdps.2012.3110.

[21] Cisco. (2019). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update (2017–2022).