Towards Design and Implementation of the Breakthrough Web

Santipong Thaiprayoon
Chair of Communication Networks
FernUniversität in Hagen
Hagen, Germany
santipong.thaiprayoon@fernuni-hagen.de

Herwig Unger
Chair of Communication Networks
FernUniversität in Hagen
Hagen, Germany
herwig.unger@fernuni-hagen.de

***Abstract*—With rising demands for accessibility, security, and privacy, the future of the Web has attracted significant attention from the digital economy, focusing on improving data protection and user experience. This article proposes a conceptual framework enabling local users to directly and safely access and share web content and services on the local and global web through their mobile devices. The local web is configured to run on a sandbox server within a specific area over a local network. In addition, the proposed framework incorporates Web 3.0, which makes the Web better understand contextual data and automatically provides personalized responses that match users. In contrast, local users retain private control over their data. The results of the experiments revealed that the proposed framework is secure, scalable, and reliable enough to be used in real-world environments. This framework could also be highly valuable in evolving the power of a decentralized Web.**

***Index Terms*—web 3.0; privacy protection; user personalization, proximity authentication, network communication.**

I. Introduction

This article is an extension of research work that was originally proposed in the Fourteenth International Conference on Advances in Future Internet (AFIN 2022) [1], which provided a personalized context-aware recommendation for the development of an autonomous intelligent agent for an individual user on online social networks.

The World Wide Web, commonly referred to as WWW, W3, or the Web, is a network system of interconnected documents and other web resources to be accessed through the Internet, linked by hyperlinks and Uniform Resource Locators (URLs) [2]. Since the Web was developed by Tim Berners-Lee, a British computer scientist, while working at CERN, the European physics research organization, it is a free "wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents." However, due to the lack of strict regulations [3], any user with a server connected to the Internet could freely and easily access and share any type of information, including texts, multimedia, and user-generated content.

As there is no connection between information and web addresses where it is stored, search engines [4] are developed to support users in an inestimable information space, and rapidly expanding social network platforms are established to connect not only content but also users in a single, worldwide-spanning system, which leads to the commercialization of the Web. Consequently, the Web has become a place that overfloods its users with plenty of useful, useless, and sometimes even dangerous or criminal information and services [5]. As a result, government institutions in all countries attempted to regulate the Internet use with many more or less valuable regulations, making Internet use sometimes more stressful than helpful [6].

In this process, users have gradually lost more and more control over what information about themselves is collected, what part of the overall available information is offered to them, and how much outdated advertising they have to tolerate. In particular, the following drawbacks can be identified:

- The Web architecture today is a centralized system of information control, which means that all personal data and user behavior are stored in a single place and controlled by one corporation or organization. This makes it easy for governments or hackers to censor content and for users to be tracked and access all of their personal information without their consent.
- Web 2.0 enables any user to publish their content in large social network systems, which is a significant improvement over Web 1.0, which only allows static linking of web pages with potentially dynamic content. However, real interaction between previously unknown users in a given context or location is still impossible. Additionally, centralized platforms can cause numerous issues for users. For instance, users are unable to quickly transfer data between platforms or switch between applications that would reuse their data.
- Information is not connected to any location or context. Typically, a web search engine returns results from any site worldwide, although that information may be senseless out of its location and context.
- The amount of information on the Web has made it difficult and time-consuming for users to find specific information. Any search engine is still a single event; previous search results cannot be refined with the help of the system. In particular, defining locations and addressing groups of people, information sources, and contexts are tedious tasks in today's search engines. Generally, the large number of search results overwhelms users, and as a result, only the top 10 to 30 results are considered, which may not be the result they prefer. The search engines should return results that are tailored to the needs of a particular user.
- Manifold data security and protection laws like the European DS-GVO [7], permanent advertisements, and push-up requests annoy users and prevent the Web from being efficient in information support. Nevertheless, it is unclear to most users what happens with their data, what meta-information is collected, and how to suppress or remove such information from third-party servers.

In conclusion, the Web of today is controlled by large corporations and governments such as Amazon, Meta (formerly Facebook), and Google. At the same time, users have to follow

their guidelines, are limited in the design of the information they offer, and need help to address it to the right, intended group of users. Moreover, the existing information flood discriminates against small information providers and merchants, which disappear in the sponsored offers of tech giants. Following Matthew Hodgson [8], "A decentralized web would give power back to the people online," also regarding their privacy, data portability, and security. However, those architectures are still not available. An additional barrier to their construction is the fact that those systems cannot be built in competition with existing structures but must be integrated into cooperating with them.

To deal with the drawbacks, a trusted conceptual framework is proposed. The proposed framework could focus on the development of personalized services and the purpose of re-decentralizing the Web by giving users complete control over personal data while managing privacy, security, transparency, and the Internet experience [9]. Additionally, users can grant or revoke access to their personal data as needed. This way enables direct interaction between users and external services hosted on local servers without intermediaries.

This article is structured as follows: In Section II, a literature review is conducted. Section III explains the architectural framework. In Section IV, communication designs are described. The experimental details are presented in Section V. Section VI contains a discussion of the results. Section VII gives examples of use cases. Finally, the conclusion and suggestions for future works are presented.

II. Literature Review

In this section, the fundamental concepts for designing and implementing the proposed framework are introduced in detail, including the evolution of the Web, Wi-Fi technology, Bluetooth technology, context-aware recommender systems, proximity authentication, user matchmaking, and user personalization. Then, related research works are discussed.

A. The Evaluation of the Web

In the early 1980s, the Internet evolved into a global communication network infrastructure that allows computer networks worldwide to connect to one another. The Internet has become an essential part of human interactions and connectivity. It enables every individual to gain access to digital information through various applications, particularly the Web. The Web is a collection of web pages containing documents and other web resources. Users can access web content via the Internet on their devices using web browsers or web-based applications [10], [11].

The development of the Web, known as Web 1.0, began in the 1990s. This is the first stage in the evolution of the Web. All Internet users are content consumers in the Web 1.0 era, where content creators provide content in web pages that are stored on web servers in the HyperText Markup Language (HTML) format. These web pages are represented as the read-only web, which consists primarily of static content and allows users to only search for and read information [12].

The lack of active interaction between users and the web pages resulted in Web 2.0. Web 2.0, the current age of the Web, is the second stage of the Web revolution. It is an improved version of Web 1.0 due to the transition from static to dynamic content that responds to user input. Web 2.0 is defined as the read-write web that emphasizes the importance of user-generated content. In the current era, any user can be both a content producer and a content consumer. With the growth of mobile technologies, they can also contribute information and communicate with other users via websites using smart devices. Meta, Twitter, YouTube, and Instagram are well-known Web 2.0 commercial platforms that allow users to contribute content, share information, and interact with other Internet users in a virtual community [13].

A large amount of new content has been currently being created and shared on Web 2.0 applications. This content information is under the control of some of the giant tech companies. This means that all of that data, including personal and sensitive data, is exploited for business purposes, such as targeted advertisements and marketing campaigns. Web 3.0 is, therefore, a concept for a new iteration of the Web that aims to make the Web more context-aware and intelligent in decentralized infrastructures. Essentially, it can understand the meaning of words and emotions through data analysis in order to automatically provide the user with highly personalized and appropriate suggestions of items by leveraging emerging technologies that heavily rely on blockchain technology, Artificial Intelligence (AI), Natural Language Processing (NLP), Machine Learning (ML), Internet of Things (IoT), Augmented Reality (AR), and Virtual Reality (VR). Users will then have a better experience driven by enhanced data connectivity. This will be achieved by empowering each user to become the owner of their data and enhancing the overall user experience through the implementation of numerous innovations. In Web 3.0, users have ownership and control over their data and can choose to share or monetize their data on their own terms. This gives users more privacy and control, addressing the concerns of data centralization and lack of privacy that are prevalent in Web 2.0. In addition, Web 3.0 enables participants to interact freely, publicly, and privately with others without the need for permission or central authorities, thus avoiding scalability and single-point-of-failure issues [14]–[16].

In summary, Web 3.0 is still a concept that is being developed. However, some businesses attempt to develop products that can be transformed into Web 3.0 applications. Some of the most widely used Web 3.0 technology can be seen in virtual assistants like Siri and Alexa and connected smart homes.

B. Wi-Fi Technology

Wi-Fi is a wireless communication technology that allows devices such as computers, mobile devices, and other equipment to interface with wireless networks [17], [18]. It is commonly used for a Wireless Local Area Network (WLAN) of devices and Internet access, allowing nearby digital devices to exchange data over radio waves. Wi-Fi technology uses radio waves to transmit and receive data between Wi-Fi devices, such as laptops, smartphones, and Wireless Access Points (APs). The radio waves used in Wi-Fi technology operate in the 2.4 GHz and 5 GHz frequency bands. These frequencies can be divided into multiple channels, and APs and Wi-Fi devices communicate over a specific channel. The channel can affect the speed and stability of the Wi-Fi connection. One of the key advantages of Wi-Fi technology is that it can support multiple devices simultaneously without needing physical cables or wires. Wi-Fi also enables multiple devices to connect to the same network, allowing users to share resources such as printers and files.

The data sent over a Wi-Fi connection is encoded using a protocol called the Institute of Electrical and Electronics Engi-

neers (IEEE) 802.11 standard. The protocol defines rules and procedures governing how Wi-Fi devices transmit, receive, and manage each other over a Wi-Fi network. The Wi-Fi protocol also includes a range of security measures to protect against unauthorized access and ensure the privacy of data transmitted over the network. Some of the security measures built into the Wi-Fi protocol include the Wired Equivalent Privacy (WEP) protocol, Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access II (WPA2) [19].

When a user needs to connect to a Wi-Fi network, the user with a Wi-Fi-enabled device begins to scan the environment for available Wi-Fi networks. It looks for APs broadcasting their network name, the SSID and determines whether the network is secured or open. If the network is open, the device can immediately connect to it, but the user will need to enter a password to gain access if it is secured. Once the device is connected to a Wi-Fi network, it starts communicating with other devices on the network [20].

Wi-Fi technology is used in a wide range of applications, from home networking to large-scale enterprise networks. In homes, Wi-Fi connects devices such as smartphones, laptops, and smart home devices. Wi-Fi is also utilized in public areas such as airports, cafes, and hotels to provide customers with free or paid Wi-Fi access [21].

C. Bluetooth Technology

Bluetooth technology is a wireless communication standard for data exchange over short distances between different Bluetooth devices, such as smartphones, laptops, and IoT devices, which attempt to build personal area networks (PANs). It allows users to simultaneously send or receive data between devices or neighboring active devices within the range of Bluetooth signals [22].

The history of Bluetooth [23]–[26] started with the first generation developed by the Bluetooth Special Interest Group (SIG) in the 1990s, which provided the Basic Rate (BR) for basic functionalities. Each new version of Bluetooth usually comes with a new mode that adds new features or makes certain things work better. In 2 and 3 generations, the SIG introduced Enhanced Data Rate (EDR) and High Speed (HS) to boost throughput in different manners, which comprised one fundamental part of Bluetooth, BR/EDR. Bluetooth Low Energy (BLE) was introduced in the four generations to increase the application fields of Bluetooth for low-power devices. Indeed, the fifth generation represents a significantly improved new generation. According to the SIG, the latest version of Bluetooth, version 5.2, which was introduced in 2019, achieved two times the transmission speed, four times the transmission range, and eight times the broadcasting capacity of Bluetooth 4.2. With Bluetooth 5.2, upgraded devices are able to transfer data more quickly and establish connections with richer content that are more stable. Currently, Bluetooth is officially successful in several areas, including speed, coverage, advertising capacity, robustness, and network capacity.

There are three primary variants of Bluetooth technology: (1) Bluetooth Classic (BC), also known as Bluetooth Basic Rate or Enhanced Data Rate (BR/EDR); (2) Bluetooth Low Energy (BLE); and (3) the recently released Bluetooth Mesh (Mesh). BC and BLE devices form a piconet in a central-peripheral manner, whereas mesh enables devices to create a mesh network based on BLE advertising.

For transferring data between two Bluetooth devices, they first establish a communication channel using a pairing process. A discoverable device should accept incoming connection requests. Generally, a device finds the discoverable device using a service discovery process. After the discoverable device agrees with the pairing request, the two devices exchange security keys to perform authentication and encryption to complete the bonding process. After the pairing and bonding processes are complete, the two devices are ready to transmit data. The security keys generated during the bonding process are reused if devices disconnect and reconnect. The two devices must always be paired and connected, with each of the two devices trusting the other and being able to exchange data in a secure manner using encryption to provide confidentiality and authenticity guarantees for communication against attackers.

In Bluetooth technology, Received Signal Strength Indication (RSSI) is a metric used to estimate the distance between two Bluetooth devices in close proximity [27]. The basic principle is that the strength of the signal decreases as the distance between the two Bluetooth devices increases. The RSSI value is measured in decibels (dBm) and indicates the power level of the received signal that reaches a device when a Bluetooth receiver is detected. Since Bluetooth receivers can broadcast their advertising packets with varying transmission power (TX) values, a combination of the RSSI and TX power values is used to estimate the distance to the device. The TX power value is the strength of the signal measured at 1 m from the device. The precision of the measured TX power value is crucial for calculating the distance between the device and the Bluetooth receiver, as the signal strength varies with the device's distance. The distance between two Bluetooth devices can be calculated using the equation (1).

$$d = 10^{\frac{TX-RSSI}{10n}} \quad (1)$$

where d is the distance in meters, and TX is an RSSI value known as the signal strength when a device and a Bluetooth receiver are at 1 meter. $RSSI$ is the device's RSSI value. The constant n depends on the location of the Bluetooth receiver or the environmental factor, ranging in value between 2 and 4.

D. Context-Aware Recommender Systems

Traditional Recommendation Systems (RS) can be modeled as a two-dimensional (2D): $Users \times Items$ space. However, considering only information about users and items is not enough in applications. Therefore, additional contextual information should be considered in the recommendation process. Contextual information includes the location, the time, the weather (e.g., the current temperature), the user's mood, the user's current activity, the user's current goals, the presence of other individuals accompanying the user, and the user's communication capabilities.

With advances in ubiquitous and mobile computing, the lack of analysis of contextual information in recommendation systems has been strongly attacked. Thus, researchers and developers have mainly focused on solving classic problems of recommendation systems, such as the cold start problem, spam vulnerability, high dimensionality, and many others [28], [29]. Recently, researchers working on recommendation systems have recognized the need to investigate them in domains where context information is relevant. In order to improve the recommendations based on contextual information, the authors extend the classical 2D paradigm to a multidimensional recommendation model that provides recommenda-

tions based on multiple dimensions: $Users \times Items \times Contexts$ space. RS incorporating context information in the recommendation process are expressed as Context-Aware Recommender Systems (CARS). In other words, CARS attempt to accommodate user preferences in various contexts. Since user preferences may vary depending on the context, it is necessary to consider context information when generating the most relevant recommendations [30]. For example, a user may prefer a different type of restaurant for a business lunch compared to a casual dinner with friends. CARS can also consider other factors, such as time of day, location, and weather conditions to provide more personalized recommendations.

E. Proximity Authentication

Proximity authentication [31]–[33] is a method of authentication that uses the proximity of a physical device, such as a smartphone or smart card, to verify the identity of a user. This method is commonly employed to enhance the security of physical access control systems, such as buildings or secure areas, or to grant access to digital resources, such as online accounts or computer systems. The basic principle of proximity authentication is that a device, such as a smartphone or smart card, is associated with a specific user and can be used to verify their identity. When a user approaches a secure area or attempts to access a digital resource, the device is brought close to a reader or sensor that can communicate with it. The reader or sensor may use a variety of technologies to communicate with the device, such as RFID, NFC, Bluetooth, or Wi-Fi. The device then sends a signal to the reader or sensor, which verifies the identity of the user and grants or denies access appropriately.

There are various research studies on proximity authentication. Zhang et al. [34] proposed a novel proximity-based authentication mechanism for IoT devices called Move2Auth. Move2Auth detects proximity by comparing the RSS trace and smartphone sensor trace during two user gestures with large RSS variations. Kalamandeen et al. [35] introduced a system that determines if two devices are in close physical proximity by taking advantage of the similarity of the channel between these devices and a third observing device. The system leverages the many devices that users already possess to aid in this process.

F. User Matchmaking

User matchmaking [36], [37] is the process of connecting users and suggesting potential matches to users with similar user profiles, interests, preferences, or goals in a digital environment. This way is commonly used in online games, dating apps, social media platforms, and other online communities where users can interact with one another. The process of user matchmaking typically involves collecting information about each user, including their age, gender, location, interests, and past behaviors. This information is then used to identify other users who are most compatible with them based on shared interests, similar activity patterns, and geographical proximity. Moreover, user matchmaking is essential for creating engaging and personalized experiences for online community users.

There are several different approaches to user matchmaking. The first approach is content-based filtering [38]–[40]. This approach involves analyzing the content of user profiles to identify shared interests or preferences. The second approach is collaborative filtering. This approach examines the behavior patterns of a large number of users to identify similarities and differences. Hybrid approaches are the third approach in that user matchmaking systems incorporate content-based and collaborative filtering to improve precision and efficiency [41]. Building a user matchmaking system requires a deep understanding of user data, such as profiles, activity histories, and behavioral patterns. This data is then analyzed using one or more of the abovementioned approaches based on machine learning algorithms to identify potential matches.

G. User Personalization

User personalization [42], [43] is the process of filtering information systems that use machine learning algorithms and data analysis techniques to identify patterns and make predictions about the user. The goal of user personalization is to suggest items or content that are tailored to the specific needs, preferences, and interests of individual users. It involves analyzing data about certain contextual situations and past behaviors of each user, such as their location, time of day, device type, search history, browsing history, purchase history, and other factors, to make relevant recommendations. In recent years, research on user personalization has been used in several fields, including e-commerce sites, social media platforms, and other online services, to suggest products, services, or content that users are likely interested in. Liu et al. [44] proposed a hierarchical framework for personalized movie recommendations. The weekly ranking of a movie is used for association and recommendation. Moreover, movie content and user preferences are integrated to generate dynamic movie synopses for personalized navigation. Yan et al. [45] proposed a personalization framework for complementary product recommendation. The model encodes user purchase history into a personalized embedding and learns product features with graph-attention networks. It is then trained jointly via a re-ranking module. Xin and Wan [46] proposed a POI recommendation model based on an improved factorization machine and BERT to extract the social, user, POI, and sequence characteristics of users.

In conclusion, user personalization is an effective way of providing users with information that is customized to their specific preferences and interests. It can help businesses to create a more personalized and engaging user experience, increasing customer satisfaction and revenue.

H. Existing Research

In the past decade, the rapid development of intelligent Web systems has been accelerated by the emergence of new Web technologies and innovative Web usage concepts. Several research studies have been reported on various application areas. Chen [47] proposed a personalized learning path generation scheme that simultaneously considers the courseware difficulty level and the concept continuity of successive courseware based on incorrect pre-testing responses while implementing personalized curriculum sequencing during learning processes. Sharma et al. [48] proposed the application of semantic web mining, focusing on web personalization. In addition to providing the user with personalized web pages, the web personalization system offers the user a list of domains in which the user may be interested. Thus, users can switch interests while searching the Internet for information. Essam et al. [49] presented a decentralized platform for social Web called Solid. Solid is a decentralized

platform for the social web that ensures data independence and simple yet powerful data management. Users store their data in Personal Online Datastores (PODs), which can be hosted on personal servers or public servers by POD providers. Users can have multiple PODs and choose from various providers based on privacy, reliability, and legal protection. Solid applications are client-side web or mobile applications that directly access and manipulate data from PODs. The platform facilitates the development and use of social features, allowing applications to aggregate data from different sources and enabling multiple applications to reuse the same data on a POD. Users can switch between applications without losing access to their existing data, as applications are decoupled from the data they use.

However, most of the existing studies ignore concerns about privacy and data protection issues for individuals who use the Web. In addition, they rarely use AI techniques to improve the performance of the Web based on the specific needs and interests of individual users in their context.

III. Architecture Framework

The Web has dramatically impacted the way people communicate, interact, and collaborate through various web-based platforms. Online users can contribute information, such as text posts, documents, videos, and photos, using computer desktops, laptops, and mobile devices. As a consequence, individuals are now able to stay connected to their local web as well as the broader global web that runs on top of the Internet using communication protocols like Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS).

The main difference between the global and local webs is their scope and accessibility. The local web is a network of websites and services that are located within a specific geographic area or physical location, like a home, office, or specific network. These websites and services typically provide information and resources to individuals within a local community. It is typically smaller and more localized than the global web, and it can be created using a variety of communication technologies such as Wi-Fi, Bluetooth, Zigbee, and others. These technologies allow devices on the local web to communicate with each other directly. This allows for faster and more reliable communication between devices and increases privacy and security. In contrast, the global web refers to the network of websites and services accessible by different individuals over a network through specific communication protocols.

One major weakness of the Web is the lack of privacy protections and accessibility for users in specific environments. This issue can be resolved by utilizing locally hosted servers, also called local servers, in a specific geographical area. It is suitable for restricted environments, such as campus networks and company intranets. The use of local servers can increase accessibility for these users by providing them faster access to information, more control over the data stored on them, and less reliance on costly and unreliable Internet connections. Similarly, local servers can keep local networks safe, which are still invisible from the Internet. Local servers can also improve security because they are less likely to be attacked or have their data stolen than commercial or global servers.

In addition, with the emergence of Web 3.0 technology, the Web is shifting towards decentralized structures that provide enhanced security, privacy, and trust. This means that users can locally store their data on their own devices or on an independent server rather than in a centralized location like Google or Facebook. The idea behind this concept is that users will have greater control over their personal information. Individual users have the ability to own and manage their personal information to preserve their privacy. Local web refers to the concept of creating and maintaining web content and services on a local level rather than relying on centralized servers. Similarly, local servers refer to using small, decentralized servers to store and distribute information rather than relying on a few large, centralized servers. Figure 1 illustrates an overview of the local and global webs for local users to access information and services.

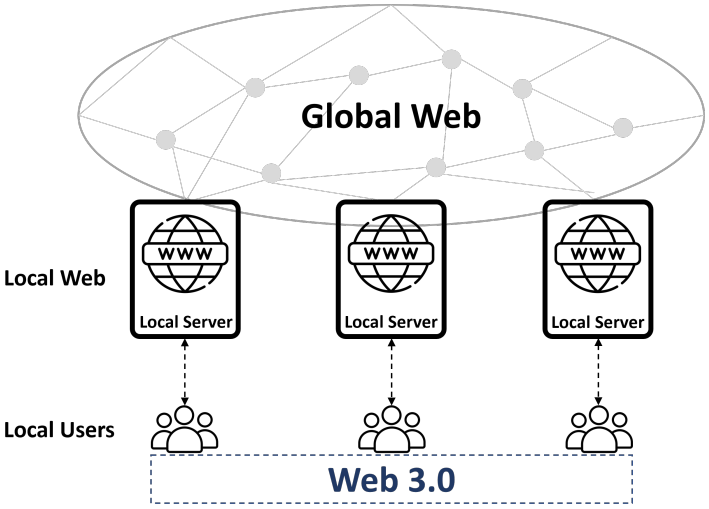

Fig. 1. An overview of the local and global web

From Figure 1, the Web can be expanded from the independent local level to the global level. Web resources are stored on a standalone local server, while they are accessed from other local servers on the Internet or public networks simultaneously. This means that each local server can securely communicate and synchronize based on HTTPS, which acts as a tunneling network. In the tunneling network, data is encrypted and encapsulated within a tunnel or secure communication channel, which is then transmitted across the network. HTTPS also uses encryption to protect data transmissions between local servers over a secure connection. Consequently, each local server enables its local users to securely and remotely participate in and access web pages or services hosted on other or neighboring local servers. The Web can be divided into two levels: (1) local web; and (2) global web. Web resources and services at the level of the local web are stored on a single local server that enables local users to access and share information about local events, news, or emergency services within a specific area. In contrast, the level of the global web is designed to be a global network system that is not controlled by any centralized servers. Web resources on several local servers are accessed by each other across that network. To describe the conceptual framework of a sandbox server in detail, the process overview is explained and illustrated in Figure 2.

A sandbox server, also called a local server, can be a physical machine or a virtual machine running on a computer connected to a local network within a sandbox environment to run applications in isolation safely. The framework is a proposed alternative approach to the current Web architecture to create a more secure

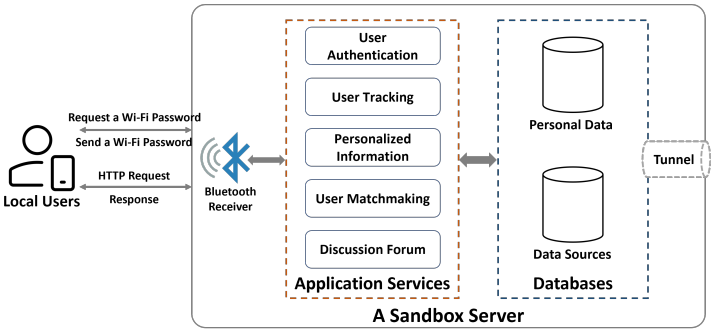

Fig. 2. The architecture framework of a sandbox server

and open Internet that prioritizes individual privacy. The proposed framework also provides a solution to privacy and data protection issues on the Web by independently separating personal data stored on mobile devices from services on local servers. Each user controls their own data through their mobile device, enabling direct interaction between users and their local server without the need for central servers. The personal data relates to an identified or identifiable natural person, including information that specifically identifies an individual, such as a name, address, telephone number, mobile number, e-mail address, credit card number, bank information, identification number, location data, or an online identifier, and information about that individual or their activities that is directly linked to the individual. The proposed framework also incorporates advanced technologies such as AI, ML, and NLP under Web 3.0 to generate personalized intelligent recommendations based on their contextual information and current vicinity, and increased privacy benefits. The proposed framework also helps prevent copyright infringement on the original works of users, such as written texts, music, images, videos, and software codes, when users publish them on the local web.

Each local user who holds a mobile device first connects to a sandbox server through a Bluetooth receiver to obtain a Wi-Fi password before accessing a local Wi-Fi network. This is a way to verify the identity of local users and protect against unauthorized access. Once the authentication process is complete, the local users are granted access to the local Wi-Fi network. Meanwhile, some of the user context stored on their mobile device is also shared and synchronized with different services on the sandbox server. These user contexts are used to identify patterns, make predictions about what the users may like, and recommend relevant information to them. The local users can then access and contribute information to the sandbox server. Furthermore, the local web can be integrated into the global web to improve accessibility and inclusivity for local users. On the level of the global web, several sandbox servers are connected across a public network, such as the Internet, to distribute access to web resources using the tunneling network that allows for the secure movement of data from one network to another. As a result, all connected sandbox servers can communicate securely and remotely with other sandbox servers and share information, services, and resources without centralized servers. Sandbox servers are autonomous and can freely join and leave the global network system at any time, which makes the system continuously and highly dynamic. For example, when a sandbox server wants to read a web page, it will look for other sandbox servers in the neighborhood that have the file and establish a direct connection between them. The file is transferred directly between the sandbox servers. One of the main benefits is that it removes bottlenecks or central points of failure from a system, as files are transferred directly over the network between two sandbox servers rather than through a central server. In addition, the proposed framework could help local users, who interact with the local and global web, identify opportunities to enhance their experiences and make the most of the resources available through the Web.

The proposed framework is designed and implemented to enable local users to access information and services on both the local and global web. Local users have the ability to have more control over their data, increase privacy, and reduce the power and authority of central servers. To explain the importance of research work, the main contributions are summarized as follows:

- A conceptual framework for the local and global web that focuses on providing information and services to local users is proposed. It enables local users to access and share information through a sandbox server and multiple sandbox servers connected together in a network, making the network more resilient and resistant to failure.
- The proposed framework can be incorporated into the global web in order to increase accessibility and inclusivity for local users.
- The local web provides more personalized and relevant results to local users based on their profiles and locations. They can be utilized to discover local information about restaurants, organizations, and opportunities for community engagement. This way can also assist in avoiding the problem of information overload.
- The combination of the local and global web is an alternative way for local users to access information from both levels of global and local information resources in different locations.
- Multiple sandbox servers operating within a network can provide benefits, such as enhanced scalability, security, and privacy, as well as the ability for local users to share resources and data directly.

In summary, the proposed framework expects to move towards becoming a web of highly intelligent interactions in the near future. It aims to rebuild the technical architecture of the Web based on the principles of decentralization. This will be accomplished through the use of artificial intelligence and communication technologies to provide Internet experiences with greater stability, security, and freedom for users, depending on their current contextual data. Moreover, the proposed framework is designed to bring power back into the hands of individuals by allowing them to own and control their data on mobile devices by utilizing the idea of peer-to-peer networks rather than companies or governments, which may use that information for their own purposes or sell it to advertisers, marketers, or others who might want access to it. This provides greater privacy and security for users, as no single entity can control what data is stored or how it can be used. It will also allow individuals to decide how much information they want to share with third parties or other people rather than having all their information stored in one place.

IV. Communication Designs

This section describes the details of the communication designs of the proposed framework. The idea behind this framework is to

provide web content and services to local users. The sandbox server is designed as an isolated environment with restricted access within a specific geographical area. Moreover, each sandbox server has the possibility to collaborate with each other via efficient ad-hoc communication. The proposed framework for a sandbox server consists of four main components: (1) application services; (2) databases; (3) Bluetooth receivers; and (4) tunneling network.

1) Application Services: These application services run on a sandbox server and provide access over a local Wi-Fi network, allowing local users to interact with the application services from a specific area and providing secure communication channels. The application services can offer specific services to local users, such as local weather and news services, which can provide dynamic content and helpful information, such as information that changes frequently or is appropriate for local users. This can help reduce the spread of misinformation and disinformation, as local users can access credible and relevant information specific to their locations and contexts.

2) Databases: This acts as a database server, providing a centralized data management platform for storing, managing, and accessing data in a database. The main role of the database server is to receive requests from the application services, search for the requested data, and return the results. In addition, this database server can hold data both temporarily and permanently. Especially, sensitive data is automatically removed after 24 hours, according to a timestamp. This provides extra security for the database, ensuring that unauthorized users cannot access sensitive data for an extended period of time. There are two databases stored on the database server, including personal data and data sources. Personal data is the collection of user data, such as name, address, date of birth, age, gender, weight, height, education, user interests, areas of expertise, and short texts from the biography. In addition, the handling of personal data by application services is governed by privacy laws and regulations, and individuals have the right to access and control their data. On the other hand, data sources refer to general raw data that is widely available through various sources, such as books, websites, and news media, typically in the form of numbers, words, images, or other forms of data. It is used to analyze data to gain a better understanding and provide users with insights and information. It can also affect privacy and security, so organizations need to be careful when collecting and using data to ensure they follow all the relevant rules and laws.

3) Bluetooth Receivers: The Bluetooth receiver acts as a terminal device for Bluetooth connections, receiving the signal from source devices, including smartphones and laptops. Bluetooth-enabled devices communicate with each other using a process called pairing. To establish a secure wireless connection, the pairing process involves exchanging information between two Bluetooth-enabled devices, such as their unique identification numbers and encryption keys.

4) Tunneling Network: This is utilized in communication networks governed by the HTTPS protocol to provide a direct connection between two sandbox servers for the security and privacy of data transmission across a public network. The HTTPS protocol operates on the basis of a client-server model. A client, such as a web browser, sends an HTTPS request to a local server, such as a web server. The local server processes the request and returns an HTTPS response to the client. The response contains data such as HTML, images, videos, and other files that can be displayed via the web browser. HTTPS uses SSL/TLS (Secure Sockets Layer/Transport Layer Security) to encrypt the transmitted data. This provides a secure channel that protects against eavesdropping, tampering, and data theft. When a client requests a web page or resource using HTTPS, the server sends its SSL/TLS certificate to the client, which verifies the certificate's authenticity and establishes a secure connection.

The main tasks of the application services consist of five services: (1) user authentication; (2) user tracking; (3) user personalization; (4) user matchmaking; and (5) discussion forum. Each service is explained in the following subsection.

A. User Authentication Service

When a local Wi-Fi network is deployed, a robust authentication mechanism is the first layer of defense for the local Wi-Fi network. Therefore, strong authentication helps to protect network access and user-sensitive data and provides security for data communications between devices on the local Wi-Fi network so that authorized individuals can only use the network. This application service proposes a scheme for Wi-Fi authentication based on Bluetooth proximity, offering an additional layer of security and functionality. When users log in to the local Wi-Fi network with Bluetooth authentication, they can access and manage data through a series of secure, encrypted connections. Proximity-based authentication is a method of authentication that relies on the physical proximity of an object or device to verify the identity of the user. The main idea of this application service is to verify the identity of local users before granting them access to the local Wi-Fi network and the resources they need based on their presence or proximity. Suppose the local users are in close enough proximity to a sandbox server. In that case, they can perform the authentication process by connecting with a Bluetooth receiver to get Wi-Fi passwords sent to their registered mobile numbers via SMS messages. In the meantime, traffic data transmitted over the local Wi-Fi network is encrypted and decrypted using the WPA2-PSK encryption standard to prevent sensitive data from leaking or being compromised. Moreover, it is a convenient way for local users with confidence to connect to the Internet through secure communications on local Wi-Fi networks effectively. The process of Wi-Fi authentication is shown in Figure 3.

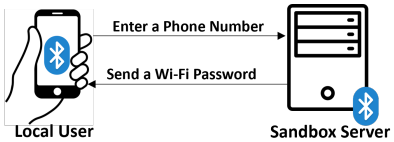

Fig. 3. The process of Wi-Fi authentication

The process begins with a local user holding a Bluetooth-enabled mobile device that attempts to connect to web content and services on a local Wi-Fi network. Before accessing the local Wi-Fi network, the local user needs to use the Bluetooth-enabled mobile device to scan for advertising signals broadcast from available Bluetooth receivers to request a Wi-Fi password. Bluetooth receivers act as devices to advertise and wait for connections, which accept an incoming connection request after advertising. When the mobile device is within the range of the Bluetooth receiver signal, it can connect and communicate with each other. The mobile device triggers an action on a mobile

application to automatically redirect to an authentication page for network access verification. Then, the local user is required to provide a phone number on the authentication page via a Bluetooth connection. Then, the sandbox server generates a Wi-Fi password and sends it directly to the registered mobile phone number of the user via SMS message. SMS is a short message containing a Wi-Fi password that is sent to the mobile phone of the local user who initiated the request. To gain local Wi-Fi network access, the local user must enter the Wi-Fi password into a captive portal authentication page on their mobile device to prove their identity. This way, it ensures that the local user accessing the local Wi-Fi network has been verified by the owner of the phone. This scheme indicates that it is extremely convenient, safe, and smooth for users, thereby enhancing their trust and confidence in using resources and services on the local Wi-Fi network.

The Wi-Fi authentication protocol relies on a combination of authentication and encryption processes to provide maximum protection for local Wi-Fi networks. The Wi-Fi authentication protocol is illustrated in Figure 4.

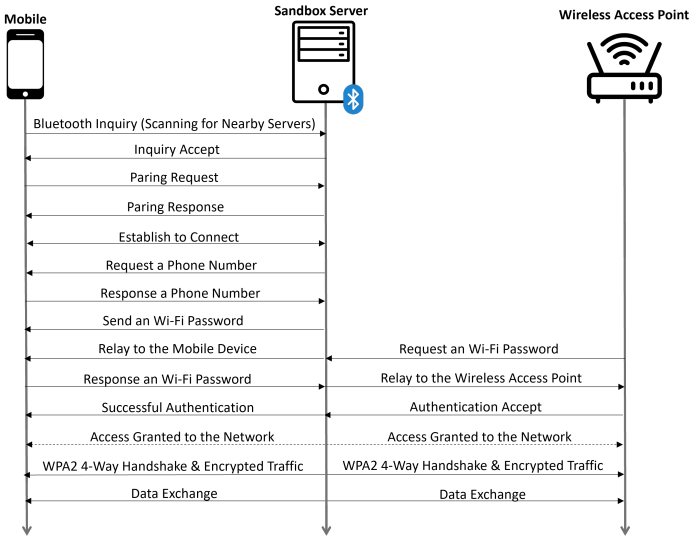

Fig. 4. The Wi-Fi authentication protocol

The user authentication process on a local Wi-Fi network performs a multi-step process involving three progressive states.

a) Registration State: A local user with a Bluetooth-enabled mobile device scans for nearby Bluetooth receivers to make a connection. After a Bluetooth receiver accepts the pairing request, the two devices complete a bonding process in which they exchange security keys. After the pairing and bonding processes are complete, the two devices exchange information. The local user then enters a phone number into an authentication web page before accessing wireless network resources. A sandbox server generates a Wi-Fi password and sends it back to the mobile phone number specified by the mobile user via an SMS message.

b) Authentication State: After the registration state is complete with a Bluetooth connection, the local user must enter the Wi-Fi password to access resources and services on the local Wi-Fi network. After authorization is complete, network access is granted to the local user.

c) Encryption State: When the authentication process is successful, the process of a WPA2 4-way handshake is performed to encrypt the data being transmitted between wireless access points and mobile devices. The local Wi-Fi network enables seamless data exchange through a single wireless access point at a time.

The Wi-Fi authentication and encryption are used in pairs to primarily prevent local Wi-Fi networks from unauthorized and malicious access attempts and secure wireless transmissions. The Wi-Fi authentication based on Bluetooth proximity acts as an interface in the middle between wireless access points and mobile devices. It helps to block all traffic except for authentication traffic. When the authentication server verifies the credentials of the user, it unblocks and permits all wireless traffic. This part could enhance the security and privacy capabilities of local Wi-Fi networks and improve the user experience.

The Wi-Fi authentication enables only the phone number owner to receive a Wi-Fi password, allowing them to log in to a local Wi-Fi network and verify their identity using a password sent via an SMS message. This makes it difficult for attackers to obtain unauthorized access to data and resources or to steal user credentials. It differs from traditional password authentication, which may continue to be useful for attackers with stolen credentials. This authentication method is an efficient way for businesses and organizations to integrate it into their authentication strategies because it has the potential to be implemented at a low total cost and directly reaches all users' existing mobile devices.

B. User Tracking Service

This application service presents a user tracking mechanism to recognize local users if they are inside a certain area based on Bluetooth technology, which is suitable for an RSSI algorithm. RSSI is a well-known location method that uses a known mathematical model that describes signal path loss with distance. The aim of this application service is to automatically determine and track local users who hold Bluetooth-enabled mobile devices and enter within the range of a Bluetooth receiver signal in real time. A sandbox server also displays that local users are present at a particular location. A Bluetooth receiver is responsible for detecting the location information of local users, tracking whether local users are still in signal coverage, and estimating the spatial distance between the Bluetooth receiver and a mobile device. The process of Bluetooth user tracking is shown in Figure 5.

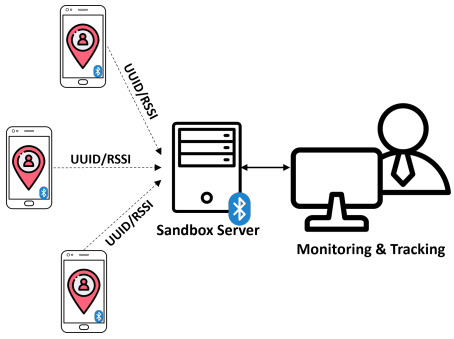

Fig. 5. The overview of user tracking

The user tracking mechanism relying on Bluetooth technology utilizes a range-based method involving the measurement of the RSSI of the Bluetooth signal from a Bluetooth receiver fixed at a prominent location. Alternatively, a fixed Bluetooth receiver is capable of calculating RSSI values transmitted by

Bluetooth-enabled mobile devices. Typically, the range-based method achieves an accuracy of a few meters and is used to determine whether an asset or a person is within a predefined room. Figure 5 demonstrates that the local users holding Bluetooth-enabled mobile devices are automatically located inside a room with a sandbox server that receives advertising messages from the mobile device. Administrators can also observe and track people staying in a specific area at a specific time to gain insight into behavioral patterns and person counts. In this case, with only one Bluetooth receiver, the local users can be roughly detected within a certain distance of the sandbox server.

On the basis of Bluetooth technology, the subsequent steps for detecting local users in a particular environment can be described.

- A fixed Bluetooth receiver starts periodically scanning advertising signals broadcasted from nearby mobile devices within the range of the fixed Bluetooth receiver signal. At the same time, each mobile device constantly advertises a Bluetooth signal containing identifying information within its range, enabling other Bluetooth devices to monitor and connect to them. When the fixed Bluetooth receiver receives Bluetooth signals from a mobile device, the mobile device is recognized as being in range. Typically, a Bluetooth broadcast signal contains a Universally Unique Identifier (UUID) and raw RSSI values. The scanning interval is set at 1000 milliseconds (1 second) to produce positioning results every second. The RSS value is measured in the unit decibel-milliwatts (dBm) and typically ranges from near 0 dBm (excellent signal) to less than -100 dBm (poor signal). A pretty value, for instance, is below -50 dBm; a reasonable value is between -70 dBm and -80 dBm, and a value of -100 dBm indicates no signal at all.
- If a mobile device appears within a specific proximity range of the fixed Bluetooth receiver signal, a Bluetooth connection between the fixed Bluetooth receiver and the mobile device is created. The mobile device is then located to determine whether it stays in a target area by measuring the signal strength with RSSI values. If the mobile device is not found, the fixed Bluetooth receiver tries to scan regularly to see whether mobile devices are present in their coverage radius. The signal strength between the fixed Bluetooth receiver and the mobile device is compared with a threshold value set at 60 dBm. If the signal strength exceeds the threshold value ($<$60 dBm), the fixed Bluetooth receiver identifies that the mobile device is in the range. If the signal strength is greater than the threshold value ($>$60 dBm), the fixed Bluetooth receiver identifies that the mobile device has moved far from the range of the fixed Bluetooth receiver. The fixed Bluetooth receiver captures a Bluetooth signal containing a raw RSSI value broadcasted from the mobile device to estimate the distance and recognize whether the mobile device is still inside the signal coverage or the targeted area.
- The fixed Bluetooth receiver roughly determines the geographical location of the mobile device by obtaining the known fixed location of the Bluetooth receiver. Then, the fixed Bluetooth receiver shows the location of the mobile device on a simple map.
- The fixed Bluetooth receiver processes the raw RSSI value from the Bluetooth network to calculate the approximate distance between the mobile device and the fixed Bluetooth receiver. Both Bluetooth devices need to be within Bluetooth range to estimate the distance. The distance between two Bluetooth devices is formulated using the equation (1).
- Administrators can continuously monitor and track the position and distance of users carrying Bluetooth-enabled mobile devices in real-time through a web-based monitoring tool.

Finally, this application service could be used to implement proximity solutions that provide location data and detect whether users enter a target area, usually within a closed environment, such as a building, shopping center, home, office, hospital, airport, conference room, or museum. Once users are identified, the system can track their location and identify them among the group of users. In addition, most smartphones are equipped with Bluetooth signal-receiving modules. Therefore, smartphones enable new Location-Based Service (LBS) capabilities. LBS provides advanced services to customers and managers, assisting individuals in determining their position. These include asset tracking, location-based advertising, business intelligence and analytics, social networking entertainment, and retail experiences.

C. User Personalization Service

The goal of this application service is to automatically provide users with the relevant information within their current situations by analyzing and understanding contextual data. A local user holding a mobile device requests and receives information and services from a sandbox server through the interface of the mobile device. The sandbox server is setup as host applications running on a web server designed to receive requests via the HTTP protocol in order to deliver static content from a website or other resources stored in a database, such as HTML, text, images, video, and other media files, to local users within a vicinity area. The content is then displayed via a web browser or mobile application. This application service of personalized information could also refer to the user tracking to deliver personalized and context-dependent recommendations of a list of relevant items based on their current location, such as nearby restaurants or shopping centers. Moreover, it allows local users to connect to the sandbox server via a local Wi-Fi network and automatically offers interesting services, such as private messages, games or puzzles, local point-of-interest, and advertising campaigns, such as promotions or discounts. This application service helps businesses enhance the user experience and improve their engagement with the product or service. This application service provides individual customers with a unique and personalized experience, allowing them to receive services that are tailored to their specific needs and preferences.

D. User Matchmaking Service

The main objective of this application service is to produce a list of potential friends with similar interests, ranked according to a similarity score based on their personal information. The matchmaking algorithm compares a user profile with other profiles using a text similarity technique and suggests a suitable list of similar users. User interests, expertise, and biographies are combined to improve the accuracy of recommending similar users. The text similarity technique measures the similarity score between two pieces of personal information based on lexical and semantic similarity, covering both word level and context level using NLP techniques, word embeddings, and cosine similarity. Each user profile is cleaned up and transformed from unstructured textual data into an appreciable format. A word embedding

technique encodes and converts textual data into a numeric format as a vector representation. Two vectors are compared using cosine similarity to extract semantically similar text from user profiles and return a similarity score.

E. Discussion Forum Service

The discussion forum is a virtual platform where individuals can come together to discuss a specific topic or set of topics. This application service is designed to facilitate online conversations and exchanges between users and can be used for a wide range of purposes. The key features of discussion forum tools include the following:

a) User Profiles: The ability for users to create personal profiles that include information such as their name, location, and interests, as well as the ability to upload profile pictures and other media.

b) Threaded Discussions: The ability for users to start new discussions or add to existing ones, creating a threaded conversation.

c) Chat: The ability for users to communicate with other users in real-time.

d) Search Functionality: The ability for users to search the discussion forum for specific topics, keywords, or posts.

e) Notifications: The ability for users to receive notifications when new content is added to the discussion forum, such as new posts, comments, or replies.

These application services have the potential to greatly enhance the customer experience, increase customer loyalty, and drive business growth.

V. Experimental Details

This section describes the experimental design for the proposed framework. The experiments are performed to evaluate the performance of local communication networks and application services to ensure the proposed framework can run in real-world use cases efficiently. The detailed experimental procedures are shown in the following subsections.

A. Experimental Strategies

The experimental strategies are divided into three strategies, including (1) Bluetooth signal testing; (2) network latency testing; and (3) application service testing. The following strategies are explained below.

1) Bluetooth Signal Testing: This strategy measures the strength and quality of Bluetooth signals between a mobile device and a Bluetooth receiver. The Bluetooth signal testing aims to estimate the range of Bluetooth signals and how they are reachable, ensure that the Bluetooth signals are stable and reliable, and support the required data transfer rate for given use cases. RSSI values captured from the signals of two Bluetooth-enabled devices are used to indicate the strength of a Bluetooth signal at a specific location. Generally, the common range of RSSI values is between -100 dBm and -20 dBm. An RSSI value of -30 dBm indicates a strong Bluetooth signal, while an RSSI value of -90 dBm indicates a weak signal. In addition, a reasonably acceptable value is -70 dBm to -80 dBm.

2) Network Latency Testing: This strategy involves measuring the time it takes for a data packet to travel from its source to its destination across a network. This measurement is expressed in milliseconds (ms). The network latency can be measured by determining the Round Trip Time (RTT), which is defined as the amount of time it takes for requested data to be transferred from a client to a server and for the server to respond to the client after the request has been processed. Ideally, the response time of network latency should be as close to zero as possible, which impacts the user experience of real-time applications, including online gaming, video conferencing, and financial trading.

3) Application Service Testing: This strategy is referred to as concurrent user testing, which assesses the performance of an application service under heavy loads, with multiple users accessing the service simultaneously for a specified amount of time. Ideally, the optimal average load time for accessing an application service is a few seconds, improving the user experience and making it easier for users to access the required information. Concurrent user testing is an important part of software testing because it helps organizations ensure that application services can perform scalability and reliability efficiently under multiple concurrent users.

These strategies could help assess the quality of application services and local network communication between a mobile device and a sandbox server and identify any issues affecting performance.

B. Experimental Setup

To show that the proposed framework is proofed and achieved, all experiments were conducted on a personal computer (PC) with an Intel (R) Core (TM) i5-4570 CPU at 3.20 GHz and 8 GB of RAM as a sandbox server in an isolated environment placed in an indoor office room with a length of 10 meters and a width of 6 meters. The Xiaomi Redmi Note 11 Pro, based on the Android 11 operating system, was used as a mobile device in all of the experimental testing. The Bluetooth receiver comes with Bluetooth version 5.0. Nginx version 1.23.3 was set up as a web server to serve dynamic web pages and web applications written in Python and Java. The backend data was stored in MySQL Server version 8.0.31, which was running on an Ubuntu 22.04 LTS Linux server.

The proposed framework was evaluated based on the three strategies mentioned above. In the Bluetooth signal testing, the mobile device and the Bluetooth receiver were used within the indoor office room to record raw RSSI values at varying distances from 1 to 10 meters. The average was calculated within a certain time frame from the raw RSSI values obtained from multiple samplings. For the network latency testing, the mobile device was set up as a client. The process starts when the client sends a data packet to the sandbox server and measures the time it takes for the sandbox server to respond. Then, the results, which contain the amount of time it takes for every packet to reach its destination and return, are used to calculate the average network latency value. The number of sending packets in each process is limited to 100. For parameter setting, the time interval of each request is set from 0.001 to 1000 milliseconds. The value of the packet size is set at 1000 bytes. For the application service testing, the testing procedure begins by simulating a large number of concurrent users accessing an application service at the same time, where the number of concurrent users ranges from 1 to

1000. The result then displays the average response time for each procedure.

VI. Results and Discussions

To verify the performance of the proposed framework, the experimental results tested on three main strategies are provided.

A. The Result of Bluetooth Signal Testing

The RSSI measurement is considered to determine the strength of Bluetooth signals. It is a metric that represents the relative quality level of a Bluetooth signal received on two Bluetooth-enabled devices. RSSI values also influence the distance range of a reliable Bluetooth connection.

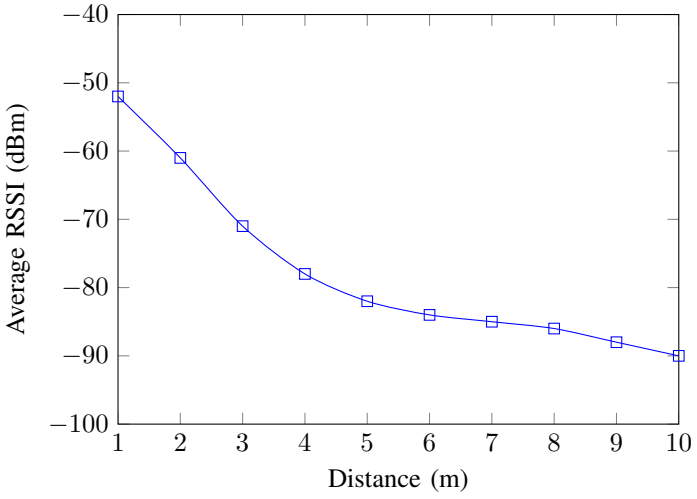

Fig. 6. The relationship between average RSSI and distance

In Figure 6, the graph demonstrates the average of the RSSI values corresponding to the different distances ranging from 1 to 10 meters. From the graph, the average RSSI values are around -50 dBm to -90 dBm. The graph is observed that the average RSSI values significantly increase when the value of the distance range is changed. Therefore, from this experimental result, the proposed framework for Bluetooth signals can support Bluetooth connections within 10 meters stably.

B. The Result of Network Latency Testing

To evaluate the network performance, network latency measurement is an important factor for network communication between a mobile device and a sandbox server.

Figure 7 shows the graph of network latency measurement using the round trip time metric by ranging the time interval from 0.001 to 1000 milliseconds. The graph indicates that the average network latency is relatively constant between 0.05 and 0.06 milliseconds for time intervals of less than one millisecond. The average network latency then gradually increases. Since the average network latency should be close to zero, it is possible to conclude from this experimental result that the proposed framework in the network connection section has the ability to quickly transfer data packets inside the pipe as they travel from client to server and back again.

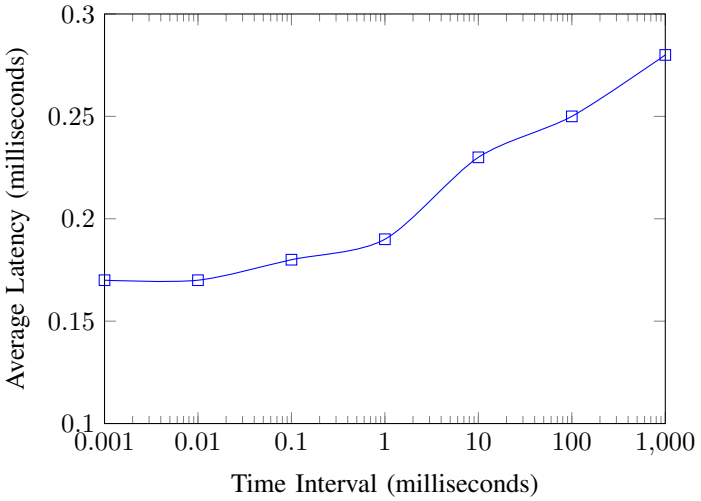

Fig. 7. The average response time with varying the number of concurrent users

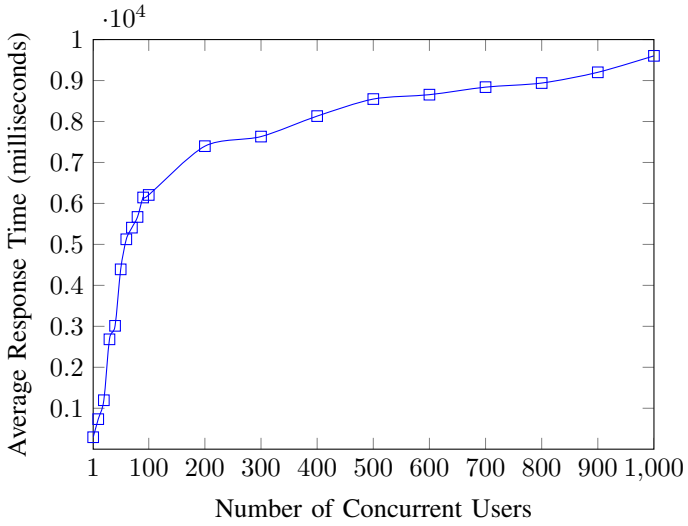

Fig. 8. The average network latency

C. The Result of Application Service Testing

To evaluate the performance of an application service running on a sandbox server under different levels of user concurrency, the metric of concurrent user testing is used.

Figure 8 shows the average response time varying with the number of concurrent users. The graph indicates that the average response time gradually increases when the number of concurrent users grows. Therefore, the number of concurrent users affects the growth of average response times because when multiple users access the application service simultaneously, they compete for the same resources, such as memory, CPU, disk I/O, network bandwidth, and database connections, which can cause system performance to degrade and increase response times. However, since the average load time should be within a few seconds, this experimental result can be interpreted as meaning that the sandbox server has enough capacity to run the application services and handles several users accessing the sandbox server efficiently.

The experimental results and proofs conclude that the proposed framework could be deployed in a production environment because it can efficiently maintain several factors at acceptable levels, including network connectivity, reliability, scalability, and

security. This means that the sandbox server is built to do different things and meet the needs of its local users. It can support many users with large amounts of data while keeping sensitive information safe and ensuring the sandbox server is not open to attack.

VII. Use Cases

In this section, a local conference room and shop located in its geographic area are examples of scenarios used to describe the storytelling and planning processes of the proposed framework. For instance, participants who enter a conference room and open a mobile application connected to a local Wi-Fi network will receive real-time information, such as a list of participants with profiles, scheduled programs, presentations, documents, videos, and any other relevant material, which will be reflected immediately in the mobile application for users who are granted access to the network. Moreover, the mobile application can be customized to allow participants to collaborate with each other, meet new friends, make comments, and share information while displaying relevant information, providing a personalized experience for each participant. Therefore, the ability to access information and interact with others through the mobile application can increase user engagement and participation at the conference. In another case, customers who enter a shop and open an application connected to the free Internet access in the venue will receive notifications on their smartphones about promotions and menu items related to the shop. This is beneficial for customers because it provides them with convenient access to valuable information. Moreover, it can also enhance the positive user experience in terms of accessibility and user satisfaction.

VIII. Conclusion and Future Directions

This article proposes a step towards a conceptual framework of the future Web that will help local users access and contribute web content and services on the local and global webs directly and safely through their mobile devices over a local network. The proposed framework is designed and implemented to run locally on a sandbox server located in a specific area to provide security, scalability, and reliability to local users. This would make the Web more secure and private for people while helping users maintain control over their privacy and avoid the risk of hacking attacks or theft. In addition, the proposed framework aims to enhance the Web evolution into an intelligent Web by leveraging the power of Web 3.0 technologies, including AI, NLP, and ML. These innovative technologies make the Web more intelligent because it can understand meaning through data analysis to automatically provide users with highly personalized and appropriate suggestions of items according to environmental contexts such as user profiles, weather, and locations. This way, the owner of their data can have great user experiences. In addition, it is crucial to consider potential legal and regulatory issues that may arise as a result of Web usage and to propose solutions to address these problems.

The future directions of the proposed framework have great potential for use in various smart environments within geographical areas (e.g., smart homes, smart universities, smart cities, and smart industries) [50]–[52]. From a home automation scenario perspective, when a user visits a home as a guest, a smart home enables the user to access and control various smart home devices via a local Wi-Fi network. When entering the home, the user must first authenticate with a proximity-based mechanism to be recognized and permitted. The user is then given access to the network and can control these smart home devices easily and safely, such as turning on the lights, air conditioners, and TVs, using an app on their phone or voice commands. When the user leaves home, he or she can no longer access and control the smart home devices. In the context of smart cities, the proposed framework could offer opportunities to fully integrate into smart cities, towns, or villages through a smartphone application to improve the overall quality of life for citizens and make their lives more efficient and convenient [53]. The mobile application serves targeted information to citizens in real time, enabling them to engage with their city. On the other hand, the proposed framework may enable city commerce to send notifications, promotions, activities, and events, which each business publishes in the mobile application, leading to increased visits. Also, all businesses get direct sales related to the offers sent.

One innovative way of using smart city apps that impact daily life is the use of navigation city tours with augmented reality technology [54], [55]. Mobile applications can help tourists visualize and navigate around cities through the lens of smartphones. The tourists receive information of interest about the history of the city and important places while walking nearby. Therefore, it is particularly useful for those cities that provide tourists with location-based augmented reality experiences using GPS coordinates.

References

[1] S. Thaiprayoon and H. Unger, "Towards personalized context-aware recommendation agent in mobile social networks," in *AFIN 2022, The Fourteenth International Conference on Advances in Future Internet*. IARIA, 2022, pp. 1–8. [Online]. Available: https://www.thinkmind.org/index.php?view=article&articleid=afin_2022_1_10_40004

[2] K. Nath, S. Dhar, and S. Basishtha, "Web 1.0 to web 3.0-evolution of the web and its various challenges," in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*. IEEE, 2014, pp. 86–89.

[3] P. J. Weiser, "The future of internet regulation," *UC Davis L. Rev.*, vol. 43, p. 529, 2009.

[4] T. Seymour, D. Frantsvog, S. Kumar *et al.*, "History of search engines," *International Journal of Management & Information Systems (IJMIS)*, vol. 15, no. 4, pp. 47–58, 2011.

[5] N. Choudhury, "World wide web and its journey from web 1.0 to web 4.0," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 6, pp. 8096–8100, 2014.

[6] D. Kaufmann, A. Kraay, and M. Mastruzzi, "The worldwide governance indicators: Methodology and analytical issues1," *Hague journal on the rule of law*, vol. 3, no. 2, pp. 220–246, 2011.

[7] C. Jaksch, "Digital personal assistants with ai and data protection gdpr & e-privacy-reg," in *Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech*. Springer, 2022, pp. 135–161.

[8] M. Hodgson, "A decentralized web would give power back to the people online," Oct 2016. [Online]. Available: https://techcrunch.com/2016/10/09/a-decentralized-web-would-give-power-back-to-the-people-online/

[9] S. Vojir and J. Kucera, "Towards re-decentralized future of the web: Privacy, security and technology development," *Acta Informatica Pragensia*, vol. 10, no. 3, pp. 349–369, 2021. [Online]. Available: https://aip.vse.cz/artkey/aip-202103-0009.php

[10] H. K. M. Al-Chalabi, "Evaluation of a multi-parameter e-learning system using web 3.0 technologies," in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2021, pp. 1–4.

[11] H. C. Salar, U. Başarmak, and M. E. Sezgin, "Educational integration of the metaverse environment in the context of web 3.0 technologies: A critical overview of planning, implementation, and evaluation," *Shaping the Future of Online Learning: Education in the Metaverse*, pp. 154–173, 2023.

[12] M. Breeding, "Web 2.0? let's get to web 1.0 first." *Computers in Libraries*, vol. 26, no. 5, pp. 30–33, 2006.

[13] K. Zdravkova, M. Ivanović, and Z. Putnik, "Experience of integrating web 2.0 technologies," *Educational Technology Research and Development*, vol. 60, pp. 361–381, 2012.

[14] R. Rudman and R. Bruwer, "Defining web 3.0: opportunities and challenges," *The electronic library*, 2016.

[15] C. Chen, L. Zhang, Y. Li, T. Liao, S. Zhao, Z. Zheng, H. Huang, and J. Wu, "When digital economy meets web 3.0: Applications and challenges," *IEEE Open Journal of the Computer Society*, 2022.

[16] F. A. Alabdulwahhab, "Web 3.0: the decentralized web blockchain networks and protocol innovation," in *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2018, pp. 1–4.

[17] K. Pahlavan and P. Krishnamurthy, "Evolution and impact of wi-fi technology and applications: A historical perspective," *International Journal of Wireless Information Networks*, vol. 28, pp. 3–19, 2021.

[18] Y. Guo, S. Zhang, and D. Xiao, "Overview of wi-fi technology," in *2012 International Conference on Computer Application and System Modeling*. Atlantis Press, 2012, pp. 1293–1296.

[19] S. Ahmed, A. N. Sakib, and S. Rahman, "Wpa 2 (wi-fi protected access 2) security enhancement: Analysis," *Global Journal of Computer Science and Technology*, vol. 12, no. 6, pp. 83–89, 2012.

[20] M. Islam and S. Jin, "An overview research on wireless communication network," *Networks*, vol. 5, no. 1, pp. 19–28, 2019.

[21] A. I. Al-Alawi, "Wifi technology: Future market challenges and opportunities," *Journal of computer science*, vol. 2, no. 1, pp. 13–18, 2006.

[22] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. Aswathy, "A state of the art review on the internet of things (iot) history, technology and fields of deployment," in *2014 International conference on science engineering and management research (ICSEMR)*. IEEE, 2014, pp. 1–8.

[23] S. Zeadally, F. Siddiqui, and Z. Baig, "25 years of bluetooth technology," *Future Internet*, vol. 11, no. 9, p. 194, 2019.

[24] S. S. Chadha, M. Singh, and S. K. Pardeshi, "Bluetooth technology: Principle, applications and current status," *International Journal of Computer Science & Communication*, vol. 4, no. 2, pp. 16–30, 2013.

[25] R. Shi, "The world of the bluetooth," in *Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021)*, vol. 12167. SPIE, 2022, pp. 161–167.

[26] J. Haartsen, M. Naghshineh, J. Inouye, O. J. Joeressen, and W. Allen, "Bluetooth: Vision, goals, and architecture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 2, no. 4, pp. 38–45, 1998.

[27] S. Chai, R. An, and Z. Du, "An indoor positioning algorithm using bluetooth low energy rssi," in *2016 International Conference on Advanced Materials Science and Environmental Engineering*. Atlantis Press, 2016, pp. 274–276.

[28] M. del Carmen Rodríguez-Hernández and S. Ilarri, "Ai-based mobile context-aware recommender systems from an information management perspective: Progress and directions," *Knowledge-Based Systems*, vol. 215, p. 106740, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950705121000034

[29] S. Raza and C. Ding, "Progress in context-aware recommender systems — an overview," *Computer Science Review*, vol. 31, pp. 84–97, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718302120

[30] Y. Zheng, "Context-aware collaborative filtering using context similarity: An empirical comparison," *Information*, vol. 13, no. 1, 2022. [Online]. Available: https://www.mdpi.com/2078-2489/13/1/42

[31] A. A. S. AlQahtani, H. Alamleh, and B. Al Smadi, "Iot devices proximity authentication in ad hoc network environment," in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. IEEE, 2022, pp. 1–5.

[32] L. Li, X. Zhao, and G. Xue, "A proximity authentication system for smartphones," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 6, pp. 605–616, 2015.

[33] A. Scannell, A. Varshavsky, A. LaMarca, and E. De Lara, "Proximity-based authentication of mobile devices," *International Journal of Security and Networks*, vol. 4, no. 1-2, pp. 4–16, 2009.

[34] J. Zhang, Z. Wang, Z. Yang, and Q. Zhang, "Proximity based iot device authentication," in *IEEE INFOCOM 2017-IEEE conference on computer communications*. IEEE, 2017, pp. 1–9.

[35] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 331–344.

[36] L. Bian and H. Holtzman, "Online friend recommendation through personality matching and collaborative filtering," *Proc. of UBICOMM*, pp. 230–235, 2011.

[37] H. Ning, S. Dhelim, and N. Aung, "Personet: Friend recommendation system based on big-five personality traits and hybrid filtering," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 394–402, 2019.

[38] T. Van Le, T. Nghia Truong, and T. Vu Pham, "A content-based approach for user profile modeling and matching on social networks," in *Multi-disciplinary Trends in Artificial Intelligence: 8th International Workshop, MIWAI 2014, Bangalore, India, December 8-10, 2014. Proceedings 8*. Springer, 2014, pp. 232–243.

[39] Z. Deng, B. He, C. Yu, and Y. Chen, "Personalized friend recommendation in social network based on clustering method," in *Computational Intelligence and Intelligent Systems: 6th International Symposium, ISICA 2012, Wuhan, China, October 27-28, 2012. Proceedings*. Springer, 2012, pp. 84–91.

[40] J. Salunke and M. A. Chaudhari, "Implementation of friendbook: a recommendation system for social networks," *Journal of Web Development and Web Designing*, vol. 29, no. 3, pp. 1–7, 2017.

[41] A. B. Barragáns-Martínez, E. Costa-Montenegro, J. C. Burguillo, M. Rey-López, F. A. Mikic-Fonte, and A. Peleteiro, "A hybrid content-based and item-based collaborative filtering approach to recommend tv programs enhanced with singular value decomposition," *Information Sciences*, vol. 180, no. 22, pp. 4290–4311, 2010.

[42] S. Y. Ho and D. Bodoff, "The effects of web personalization on user attitude and behavior," *MIS quarterly*, vol. 38, no. 2, pp. 497–A10, 2014.

[43] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, pp. 203–220, 2012.

[44] A. Liu, Y. Zhang, and J. Li, "Personalized movie recommendation," in *Proceedings of the 17th ACM International Conference on Multimedia*, ser. MM '09. New York, NY, USA: Association for Computing Machinery, 2009, pp. 845–848. [Online]. Available: https://doi.org/10.1145/1631272.1631429

[45] A. Yan, C. Dong, Y. Gao, J. Fu, T. Zhao, Y. Sun, and J. Mcauley, "Personalized complementary product recommendation," in *Companion Proceedings of the Web Conference 2022*, ser. WWW '22. New York, NY, USA: Association for Computing Machinery, 2022, pp. 146–151. [Online]. Available: https://doi.org/10.1145/3487553.3524222

[46] M. Xin and C. Wan, "Poi recommendation algorithm for mobile social network based on user perference tracking," in *The 2nd International Conference on Computing and Data Science*, 2021, pp. 1–7.

[47] C.-M. Chen, "Intelligent web-based learning system with personalized learning path guidance," *Computers & Education*, vol. 51, no. 2, pp. 787–814, 2008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360131507000978

[48] A. Sharma, "Semantic web mining for intelligent web personalization," *Journal of Global Research in Computer Science*, vol. 2, no. 6, pp. 77–81, 2011.

[49] E. Mansour, A. V. Sambra, S. Hawke, M. Zereba, S. Capadisli, A. Ghanem, A. Aboulnaga, and T. Berners-Lee, "A demonstration of the solid platform for social web applications," in *Proceedings of the 25th International Conference Companion on World Wide Web*, ser. WWW '16 Companion. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2016, p. 223–226. [Online]. Available: https://doi.org/10.1145/2872518.2890529

[50] C. Yin, Z. Xiong, H. Chen, J. Wang, D. Cooper, and B. David, "A literature survey on smart cities." *Sci. China Inf. Sci.*, vol. 58, no. 10, pp. 1–18, 2015.

[51] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable cities and society*, vol. 38, pp. 697–713, 2018.

[52] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *The European Physical Journal Special Topics*, vol. 214, pp. 481–518, 2012.

[53] A. Hoadjli and K. Rezeg, "A scalable mobile context-aware recommender system for a smart city administration," *International Journal of Parallel, Emergent and Distributed Systems*, vol. 36, no. 2, pp. 97–116, 2021. [Online]. Available: https://doi.org/10.1080/17445760.2019.1626855

[54] P. Yagol, F. Ramos, S. Trilles, J. Torres-Sospedra, and F. J. Perales, "New trends in using augmented reality apps for smart city contexts," *ISPRS International Journal of Geo-Information*, vol. 7, no. 12, p. 478, 2018.

[55] S. Kaji, H. Kolivand, R. Madani, M. Salehinia, and M. Shafaie, "Augmented reality in smart cities: applications and limitations," *Journal of Engineering Technology*, vol. 6, no. 1, pp. 28–45, 2018.