ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 7, Num. 2, 2022

WIFIZONECLOUD: A CLOUD-BASED WI-FI HOTSPOT PLATFORM

Busra Ozdenizci Kose[1], Senol Yaya[2], Vedat Coskun[3]and H. Ali Mantar[4]

[1]Gebze Technical University, Kocaeli, Turkey.
[2]Turcom Technology, Istanbul, Turkey.
[3]Atlas University, Istanbul, Turkey.
[4]Gebze Technical University, Kocaeli, Turkey.

Authors' e-mail*: [1]busraozdenizci@gtu.edu.tr, [2]yayas@turcom.com.tr, [3]vedat.coskun@atlas.edu.tr, [4]hamantar@gtu.edu.tr*

Submitted on 09.07.2022

***Abstract*: Today, there are millions of Wi-Fi hotspots available by diverse service providers such as operators, public spaces, enterprises, and even cities. With the developments on OpenRoaming approach, cloud federation, automatic global roaming, efficient user onboarding and network automation have become important requirements for stakeholders within the ecosystem. This study aims to present a cloud based hotspot platform solution called WifiZoneCloud which enriches the limited hotspot capabilities of new generation firewall, access point and similar network devices; provides roaming between different locations of an institution; keeps the use of the network under control and makes the network reportable, and even performs required logging. With diverse authentication tools, the platform ensures high security according to the needs of users. Above all, these operations are completely administered in the cloud environment. The proposed new platform is likely to pave the way for the establishment of the global Wi-Fi network and present valuable opportunities in the 5G era.**

***Index Terms*: Hotspot, OpenRoaming, cloud, network, user management, traffic monitoring.**

I. INTRODUCTION

A hotspot can be described as "a physical location where people can access the Internet, typically using Wi-Fi, via a wireless local area network (WLAN) with a router connected to an Internet service provider" [1]. These locations are generally named as "Wi-Fi hotspots" which refers to the IEEE 802.11 communications standard for WLANs [2]. Basically, hotspots are the physical areas where users can wirelessly connect their smartphones, tablets and other Internet capable devices. A hotspot can be in a private or a public location, such as in a hotel, an airport, or in a shopping mall. While some public hotspots provide free wireless access, some of them require payment [3][4]. Wi-Fi hotspots are largely similar, there are a few different types available, and they have some distinct differences.

Today, there are millions of Wi-Fi hotspots available by diverse providers such as operators, venues, public spaces, enterprises, cities and so on [5]. As highlighted by the report of Cisco, the number of global Wi-Fi hotspots is expected to reach over 600 million by 2023 [6]. From user's perspective, connecting to public Wi-Fi networks sometimes becomes a tedious and inconvenient experience [5]. This process repeats each time when users try to access a different Wi-Fi network. Moreover, this situation creates fragmentation and making it impossible to build a Wi-Fi roaming service at any scale [5].

Accordingly, in May 2020, the Wireless Broadband Alliance (WBA) launched OpenRoaming which is an effort to address the fundamental Wi-Fi connectivity issues [7]. This roaming federation service aims to enable an automatic and secure Wi-Fi experience globally and to create an open connectivity framework for all organizations in the wireless ecosystem [7]. It brings together Wi-Fi Access Network Providers (ANPs) and Identity Providers (IDPs) under a Public Key Infrastructure (PKI) based model. As it is highlighted in [7], WBA OpenRoaming standard focuses on three key elements: (1) Cloud federation to enable automatic roaming and user onboarding on Wi-Fi; (2) Cyber Security to enable simple, secure and scalable Wi-Fi connections among different organizations that are part of WBA OpenRoaming; and (3) Network automation to define an automated roaming consortium codes framework (RCOI) to support policy provision on devices and networks. Currently, WBA OpenRoaming Wi-Fi roaming standard is supported by many high-profile companies such as AT&T, Boingo, Broadcom, Cisco, Commscope, Deutsche Telekom, Facebook, Google, Intel, Net Experience and Samsung.

In recent years, significant developments on cloud technologies have led network hardware manufacturers to develop their own value-added products and services. They aimed to make the devices they produce manageable in the cloud environment. Particularly in the field of Wi-Fi hotspot solutions, with the developments on OpenRoaming approach, cloud technologies have become an important issue for many network hardware manufacturers. There is a wide variety of local and cloud-based Wi-Fi hotspot platform solutions for providers. However, local solutions are very difficult to manage and have problems with updating processes. On the other hand, recent cloud-based solutions are created by

targeting the products of a certain brand and it is observed that there is no flexibility of customization.

This study aims to present an innovative cloud hotspot platform solution called WifiZoneCloud which enriches the limited hotspot capabilities of new generation firewall, access point and similar hotspot capable devices; keeps the use of the network under control and makes the network reportable, and even performs required logging. The proposed infrastructure is located completely in the cloud environment to make the endpoint user independent from hardware and infrastructure resources. It enables to control, analyze and report the internet usage of in-house guest internet users. Thus, using the cloud hotspot capabilities of network hardware manufacturers, different authentication methods are also offered to customers, and the information received from these networks can be analyzed and reported.

The rest of this paper is organized as follows: Section II presents the methods for designing and developing WifiZoneCloud platform. Section III explains how the system platform works. Finally, the study is concluded in Section IV.

II. METHODS

WifiZoneCloud platform can be used by service sector, convention and culture centers, municipality subsidiaries, public institutions, mass transportation vehicles, entertainment sector, chain businesses and any institution which open its internet services to general use and which have the liability to inform such as institutions rendering service as any type of "hotspot". With the help of WifiZoneCloud platform, these actors can use the capabilities of their own devices in their network infrastructure more efficiently in terms of hotspot, user management, traffic monitoring and network management.

A. DESIGN CONSIDERATIONS

The main design issues of WifiZoneCloud platform are described under three headings:

(1) Creating Manageable Guest Networks on the Cloud: Network administrators will be able to manage, report and analyze in-house hotspot networks from any location. These services are currently provided with in-house hotspot devices. In addition, it creates a limiting factor for the customer, as the structures working in similar examples working in the cloud environment are dependent on a certain hardware. With the ability of the proposed platform to work in the cloud environment, the obligation of the customer to open the local network to the external environment is eliminated. All network equipment with hotspot capability will be supported. Thus, it will be ensured that the customer is not obliged to a certain equipment.

(2) Building Global Roaming Capability: Users with more than one location are provided with the opportunity to login with the same information as other locations after logging in only once. Currently, since each location has a separate user portfolio, Users are required to re-register at different locations. This creates unnecessary costs for our customers and negatively affects the end user experience. With global roaming capability, the platform makes a difference compared to its peers.

(3) Enriching Authentication Process by Using Different Methods: Apart from the standard authentication form where users only log in with a username and password, authentication methods that may include different integrations that they can shape themselves will also be presented. Existing solutions generally have only the ability to verify only via SMS. With WifiZoneCloud platform, various authentication models will be performed according to the login parameters that the user will define on the administration screen.

B. SYSTEM DEVELOPMENT

For the development of WifiZoneCloud platform, following issues have been considered:

(1) Using the Hotspot Capability of Network Devices: Network equipment with external hotspot capability will be able to be directed to the customized hotspot login page by interfering with the internet traffic of the users connected to the network.

(2) Use of Authentication Servers: Due to their nature, hotspot systems need Radius (Remote Authentication Dial In User Service) servers for authentication. Radius is the software that provides authentication service to the hotspot service by keeping the user and user limit information needed for the hotspot. In our system, it is aimed to provide hotspot system authentication service by using more than one Radius server with a road balance structure.

(3) Use of MySQL Database: MySQL database will be used to provide infrastructure to Radius servers and customized hotspot structures. The purpose of choosing MySQL database is that Radius servers work more efficiently with MySQL database and resource usage in Linux infrastructure is more optimized.

(4) Infrastructure: Linux operating system will be used for all systems to run on it. Linux was preferred because of the more optimized resource usage.

C. AUTHENTICATION MODELS ON WIFIZONECLOUD

User authentication and verification tools are essential design issue of Wi-Fi hotspot solutions. With WifiZoneCloud platform, diverse authentication tools are designed in a modular structure. In this way, desired authentication tool can be added or removed via the administration panel depending on the user company's preference.

The methods to be presented in the administration panel of WifiZoneCloud platform are as follows:

(1) Static Method: No information is requested from the user. By clicking the login button on the welcome page, the user is allowed to use the internet.

(2) Standard Method: Users are created manually from the management interface by the administrator and users can log in with the username and password given to them on the welcome screen.

(3) SMS Method: It is the method where users can register with a registration form and log in with the username and password sent to them.

(4) VIP Method: It is the method that allows internet use without the need for any welcome screen defined by the administrator.

(5) Active Directory (AD) / Lightweight Directory Access Protocol (LDAP) Method: AD is a directory service developed by Microsoft for Windows domain networks [8]. This service stores information about user accounts, such as names, phone numbers, passwords, and many other credentials. Also, it enables authorized users on the same network to access this sensitive information. On the other side, LDAP is the lightweight version of the Directory Access Protocol [9]. It is an open industry standard mechanism and a cross platform protocol for interacting with directory servers; namely it is used for directory services authentication. This service on WifiZoneCloud platform enables users to log in by integrating the user information registered in the AD/LDAP structure of the institution.

(6) Interactive SMS Method: It is a service where the user can use the internet by sending a random code given on the welcome screen to a specific GSM number [10] [13]].

(7) XML Method: This allows the user to verify over a requested XML Web Service.

(8) PMS Method: It is the method in which WifiZoneCloud verifies user information integrated with the institution's registration system, and the information used by the institution for authentication is requested from the user (surname/room no, identity/room no etc.). This service is generally suitable for use in hotels.

(9) OAuth2 Method: This service allows the user to be authenticated by integrating with systems using the OAuth 2.0 authentication standard [14] such as Facebook, Twitter, Google etc. OAuth 2.0 Authorization Protocol (Fig. 1.) is the access and sharing of the information (owned by the Resource Owner and managed by the Resource Provider) by the service provider under control of authentication server [15] [16].

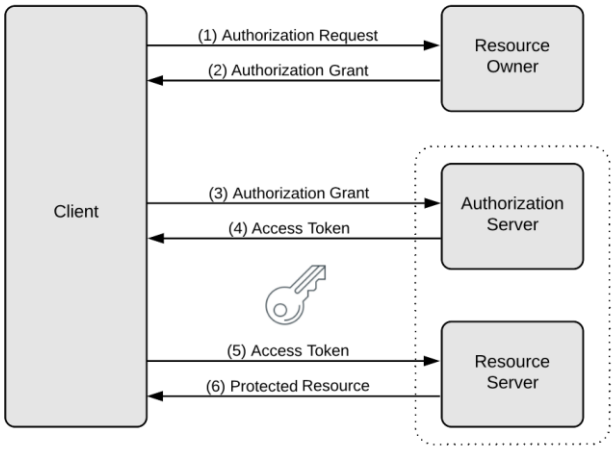


Fig. 1. OAuth 2.0 General Protocol Flow [14] [15]

III.HOW WIFIZONECLOUD WORKS

A. HOTSPOT FEATURE

(1) Network Device Side: The next generation network devices in the network that will use the WifiZoneCloud system have the ability to define Hotspot and Radius servers.

All definitions related to the functioning of the hotspot capability are made on the relevant network device. These configurations vary according to the manufacturer and model, but basically there are areas where the definitions of the hotspot page are provided. In order to run the WifiZoneCloud system, the URL produced by the WifiZoneCloud system is defined in these configurations.

The URL is defined in the same way as the Radius server, and ports 1812 and 1813 are defined for access and accounting transactions. Radius Access is the first login request that the user sends to the authentication server. Radius Accounting is the radius package in which the user's usage information on the network is transmitted in a certain period within the framework of the configuration on the hotspot server after the user connects over the hotspot.1812 is used for access Radius packages and 1813 is used for accounting Radius packages.

SSID (service set identifier) and DHCP (Dynamic Host Configuration Protocol) definitions are made on the network device independently of the hotspot. These definitions are assigned to the network defined for the hotspot. SSID is the sequence of characters that uniquely names a WLAN. An SSID is sometimes referred to as a "network name." This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area. The user chooses it from his device to connect to the wireless network. DHCP is the network management protocol service used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.

(2) WifiZoneCloud Side: In case of management flow, the customer, who has a new generation network device and wants to use the system, logs in to the system by registering in the system and adds her institution's or company’s information to the system (Fig. 2) and manages different locations as well.

After this stage, it defines the web URL where the hotspot service will be provided by creating a subdomain under WifiZoneCloud domain or a subdomain under its own domain for the hotspot page it wants to create.

After the URL is defined, the manager determines the authentication method (SMS, PMS, etc.) that she wants to use in the hotspot system (Fig. 3).

The manager can customize the hotspot page according to her institution. After login, she can determine the web URL she wants to be accessed. By connecting the users using the form to the user groups it defines, it can provide access to the internet with certain quotas (speed, data, time). In addition to user management, the manager can monitor all the devices on the network (Fig. 4). A real-time summary data is shared on the dashboard of administration panel for manager (Fig. 5).

On the other side, the user connects to the SSID defined by the institution for the hotspot, and then is directed to the hotspot address by the network device. This is the URL defined by the page manager. When she accesses the URL,

she registers using one of the authentication forms defined by the manager and enters the information provided to him in the form and presses the "Login" button.

The information received from the user is sent to the Radius verification address of the network device. The network device receiving the information converts the data into a Radius information packet to send the data to the Radius server and transmits it to the WifiZoneCloud server defined on it via port 1812.

After the user's presence has been checked on the Radius server, the access limits are taken and sent to the network device. Access is provided to the user requesting connection within the framework of these limits.

After the access is granted, if the manager has defined a domain for routing the user, if the user has not defined the defined domain, they are directed to the address they want to access.

B. LOGGING FEATURE

Some countries have laws to control internet access and prevent illegal activities; The responsibilities of the line owners and the technical actions to be taken have been determined. Within the scope of these transactions, line owner organizations are responsible for internet access on the line and must keep records within the framework of certain rules.

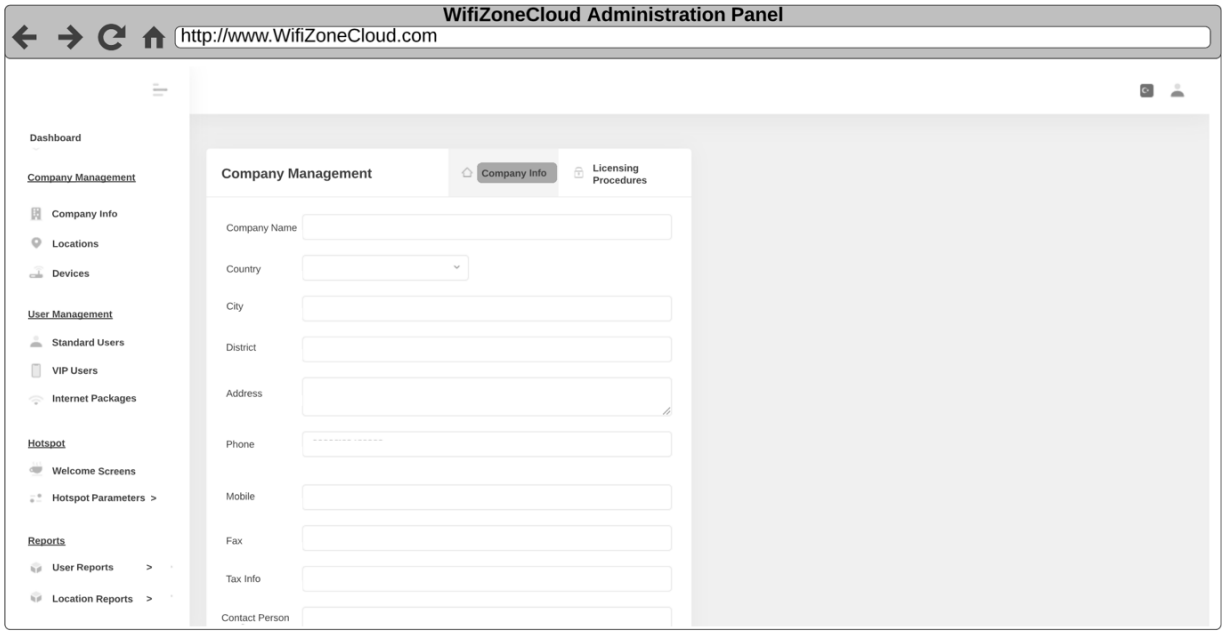


Fig. 2. WifiZoneCloud Administration Panel – Company Management UI

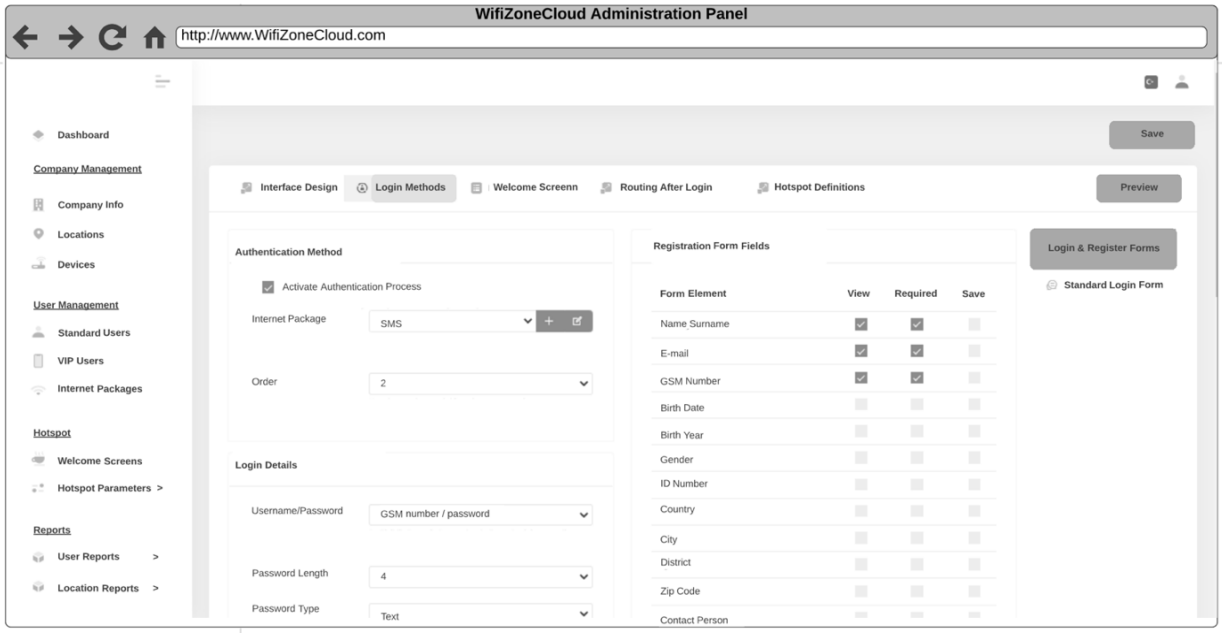


Fig. 3. WifiZoneCloud Administration Panel – Authentication Setting UI

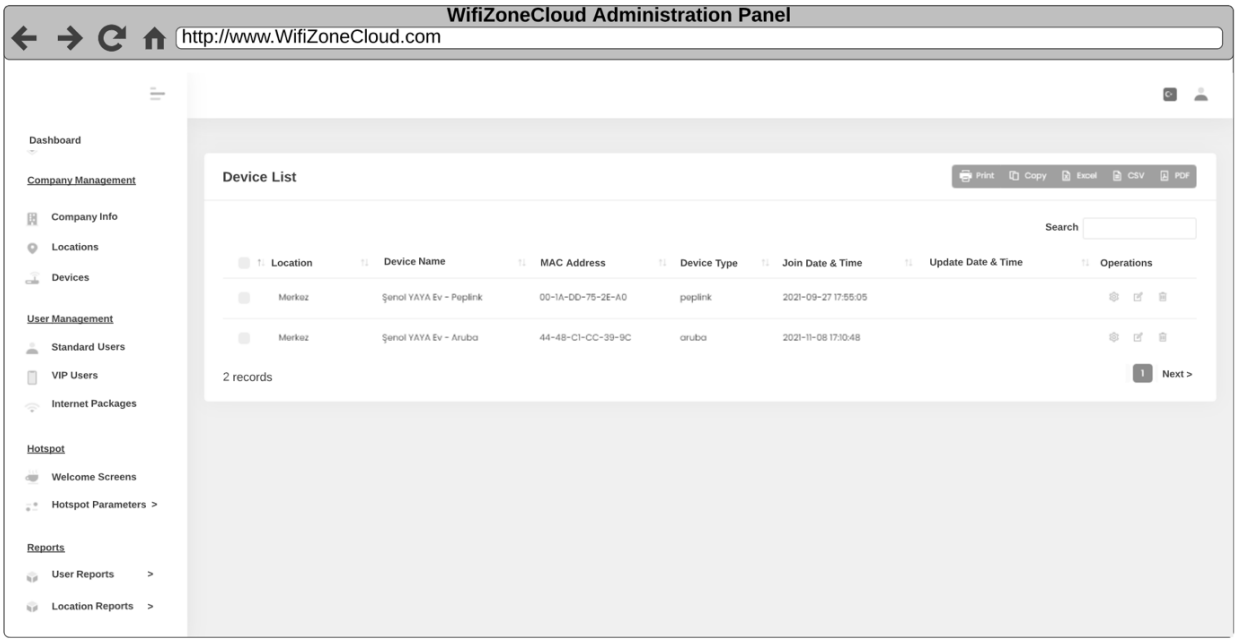


Fig. 4. WifiZoneCloud Administration Panel – Device Management UI

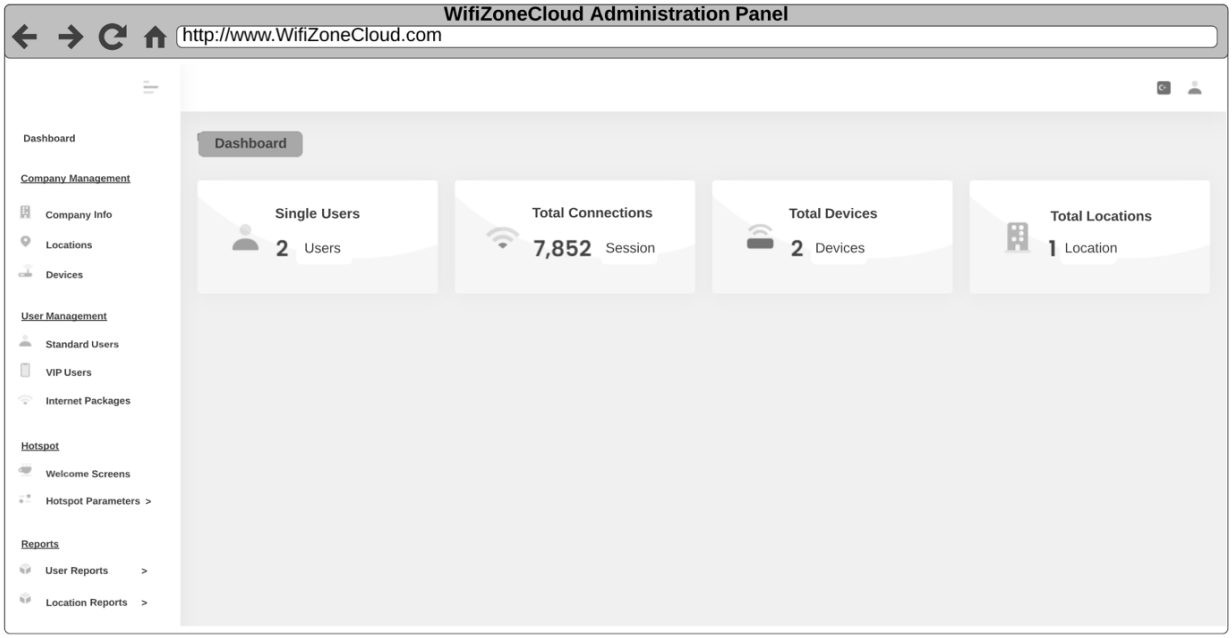


Fig. 5. WifiZoneCloud Administration Panel – Dashboard UI

It is ensured that the unique access information of the accessing user is kept under record. Each session of the users registered within the scope of WifiZoneCloud is recorded separately between the start and end intervals. In this context, the user's name, surname, GSM number, e-mail, etc. information is retrieved and logged by matching the unique information with the session record. At the same time, it is ensured that the user's web access logs are kept. Web access logs, known as access logs, are recorded by matching the user's unique log information. Provided access and usage logs are signed and archived daily by nationally accepted digital signature service providers.

B. ROAMING FEATURE

With the advantage of working in the cloud environment, WifiZoneCloud can provide internet access at different points of the institution around the world without the need for users to re-register. At the same time, if the device of the managed institution can provide Radius access at layer 2 level, direct internet access will be provided when the user connects to the network without encountering the hotspot welcome screen.

C. REPORTING FEATURE

Through the logs obtained from the user's access, data such as whether the users are successful with the information they

use to log in, instant data traffic, the addresses they access, the devices used while accessing, and session information can be reported.

IV. CONCLUSION

This study presented the basics of a manageable hotspot system in the cloud environment. The new platform will benefit three main entities within the ecosystem:

(1) Device Manufacturers: Complex device tuning can be done via the WifiZoneCloud platform with more than 95% performance. Customized authentication processes, guest network management, reporting and analysis capabilities, which they cannot provide in their own infrastructure, will be gained.

(2) Customers: They can manage technical and complex processes such as Internet access and device setup via the platform with at least 90% reliability and robustness. This means that it will be easier to manage, customize, report and analyze guest networks in line with their needs.

(3) Government Agencies: Internet traffic information, which must be kept as per the law, will be kept totally. By recording and signing HTTP and DHCP logs by the system, customers can fulfill their responsibilities to the government without any problems.

The development stage of the WifiZoneCloud platform is currently almost complete. After development and dissemination stages, WifiZoneCloud platform is expected to support almost all the basis of establishing a worldwide Wi-Fi network with the developing wireless technologies. It will enable end users to easily register for each Wi-Fi internet access point and automatically join each access point in a very short time (approximately <30 seconds) with considerable ease. Besides, it will be possible to set up many Internet access point devices, enable end-users to join the platform securely with their personal devices, and ensure that all transactions during the session are conducted by security standards.

References

[1] Intel (2022). What Is a Hotspot? - WiFi Hotspot Definitions and Details. https://www.intel.com/content/www/us/en/tech-tips-and-tricks/what-is-a-hotspot.html (Accessed: 08 July 2022).

[2] Henry, P. S., & Luo, H. (2002). WiFi: what's next?. *IEEE Communications Magazine*, *40*(12), 66-72. DOI: 10.1109/MCOM.2002.1106162

[3] Seufert, M., Griepentrog, T., Burger, V., & Hoßfeld, T. (2015). A simple WiFi hotspot model for cities. *IEEE Communications Letters*, *20*(2), 384-387. DOI: 10.1109/LCOMM.2015.2509074

[4] Korn, M., & Klokmose, C. N. (2012, September). Putting 'local' back into public Wifi hotspots. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 800-801). DOI: 10.1145/2370216.2370399

[5] Canpolat, N. OpenRoaming: One Global Network of Wi-Fi Network. *Wireless Systems Global Connectivity*. https://www.intel.com/content/dam/www/central-libraries/us/en/documents/wi-fi-open-roaming-overview-whitepaper.pdf (Accessed: 08 July 2022).

[6] Cisco Annual Internet Report 2020, https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html (Accessed: 08 July 2022).

[7] WBA OpenRoaming, https://wballiance.com/openroaming/ (Accessed: 08 July 2022).

[8] Iyer, N. C., Kabbur, A. M., & Wali, H. G. (2020). Implementation of Active Directory for efficient management of networks. *Procedia Computer Science*, *172*, 112-114. DOI: 10.1016/j.procs.2020.05.016

[9] Koutsonikola, V., & Vakali, A. (2004). LDAP: framework, practices, and trends. *IEEE Internet Computing*, *8*(5), 66-72. DOI: 10.1109/MIC.2004.44

[10] Ozdenizci Kose, B., Cevikbas, C., Mantar, H.A., Buk, O., Coskun, V. (2020, September). Design of a Secure Key Management System for SIM Cards: SIM-GAYS. In *2020 5th International Conference on Computer Science and Engineering (UBMK)* (pp. 388-392). IEEE. DOI: 10.1109/UBMK50275.2020.9219504

[11] Ozdenizci Kose, B., Morkoyun, S.E., Alsadi, M., Mantar, H.A., Coskun, V. (2019, October). A SIM Card Based Key Management System. In Proceedings of International Conference on Advances in Business Management and Information Technology (ICABMIT'19), (pp. 1-5).

[12] Ozdenizci Kose, B., Cevikbas, C., Mantar, H.A., Coskun, V. (2020). Development of a SIM Card based Key Management System. *European Journal of Science and Technology*, (Special Issue), 70-77. DOI: 10.31590/ejosat.818711

[13] Ok, K., Coskun, V., Yarman, S. B., Cevikbas, C., Ozdenizci, B. (2016). SIMSec: A key exchange protocol between SIM card and service provider. *Wireless Personal Communications*, 89(4), 1371-1390. DOI: 10.1007/s11277-016-3326-5

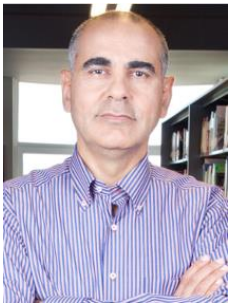
[14] OAuth 2.0, https://oauth.net/2/ (Accessed: 08 July 2022).

[15] Ozdenizci Kose, B., Buk, O., Mantar, H. A., & Coskun, V. (2020, October). TrustedID: An Identity Management System based on OpenID Connect Protocol. In *2020 4th International IEEE Symposium on Multidisciplinary Studies and Innovative Technologies* (pp. 1-6). DOI: 10.1109/ISMSIT50672.2020.9254886

[16] Ozdenizci Kose, B., Buk, O., Mantar, H. A., Coskun, V., & Erdemir, U. (2021). Protecting Mobile Service User Identity by Adding Additional Security Layer. *European Journal of Science and Technology*, (23), 22-30. DOI: 10.31590/ejosat.833433

Dr. Busra Ozdenizci Kose received M.Sc. degree at the Department of Information Technology in Isik University and Ph.D. degree at Informatics Department in Istanbul University. She co-authored the books titled ''Near Field Communication: From Theory to Practice'' published by John Wiley & Sons, Inc., 2012 and ''Professional NFC Application Development for Android'' published by Wrox, 2013. Her research areas include Near Field Communication, Smart Cards, Mobile Communication Technologies and Blockchain.

Senol Yaya is an Engineer. He works as the R&D Manager in TURCOM Technology, Turkey. He focused on various technologies such as Internet of Things, Linux systems, and Agile Software Development.



Prof. Dr. Vedat Coskun is a Computer Scientist, Academician, Researcher, and Author. He is founder and manager of NFC Lab—Istanbul (www.NFCLab.org), the pioneer research lab on Near Field Communication technology worldwide. He is currently a Professor of Information Technology in Beykent University, Istanbul. He is specialized and teaches courses in a wide range of topics such as Blockchain, Cybersecurity, Cryptography, Algorithms, Python, Java, and Javascript Technologies, and Near Field Communication. He delivered lectures in several universities all around the World. He believes on the importance of academia & industry relationship in Information Technology, and takes such roles as project development, researcher, and consultant for national and international companies in this manner.

Prof. Dr. H. Ali Mantar received his B.Sc. degree in Electronics and Telecommunication Engineering at Istanbul Technical University (1993), received his M.Sc. and Ph.D. degrees in Electrical Engineering (1998) Computer Science (2003) at Syracuse University. He worked as a lecturer at Syracuse University between 1997 and 2000. His research work was supported by the Graduate Students Research in Wide Area Network Management project which was funded by the National Science Foundation (NSF) and was involved in a Computer Resilience Project funded by DARPA, USA (2003-2005). He worked as a Professor of Computer Engineering at Gebze Technical University (2004-2006), Director of TÜBİTAK - BİLGEM (2015-2020), and Istanbul Technical University Vice Rector (2021-2022). He is acting as the Rector of Gebze Technical University.