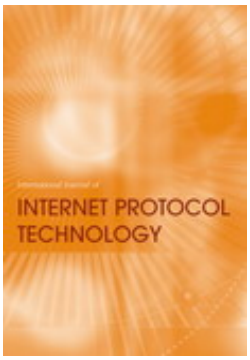


International Journal of Internet Protocol Technology

ISSN online: 1743-8217 - ISSN print: 1743-8209
https://www.inderscience.com/ijipt

Near field communication-triggered wireless local area network authentication

Vincent R. Sarmiento, Yna Maxene P. Campana, Benedick San Gabriel, John Joshua F. Montañez

DOI: 10.1504/IJIPT.2024.10068478

Article History:

Received:	11 June 2024
Last revised:	23 November 2024
Accepted:	24 November 2024
Published online:	06 January 2025

Near field communication-triggered wireless local area network authentication

Vincent R. Sarmiento,
Yna Maxene P. Campana
and Benedick San Gabriel

Department of Electronics Engineering,
College of Engineering,
Bicol State College of Applied Sciences and Technology,
Peñafrancia Avenue, Naga City, Camarines Sur, Philippines
Email: vrsarmiento@astean.biscast.edu.ph
Email: ympcampana@astean.biscast.edu.ph
Email: bsangabriel@astean.biscast.edu.ph

John Joshua F. Montañez*

Intellectual Property Management Office,
Department of Electronics Engineering,
College of Engineering,
Bicol State College of Applied Sciences and Technology,
Peñafrancia Avenue, Naga City, Camarines Sur, Philippines
Email: jjfmontanez@astean.biscast.edu.ph
*Corresponding author

Abstract: User authentications has become a necessary part of every communication protocol. There is a boundary between security and user convenience when authenticating. Near Field Communication (NFC) is a tool for interfacing connections. This was implemented through software and hardware development of the network to handle database and dedicated login credentials for each user when connecting to a wireless network. WPA/WPA2 Enterprise Authentication was used with Remote Authentication Dial-in User Service (RADIUS) to create the network. NFC-implemented authentication was compared with traditional authentication regarding speed and security vulnerabilities. Results from the tests conducted have shown significant improvement in using NFC as a means to bring more convenience to the authentication process, garnering an average speed of 9.82 seconds compared to the traditional one, having high variability depending on different password lengths, having an average 19.5 seconds and an increased average of 9.55 seconds for every eight additional characters to the password.

Keywords: near field communication; radio frequency identification; remote authentication dial-in user service; Wi-Fi; WPA; Wi-Fi protected access.

Reference to this paper should be made as follows: Sarmiento, V.R., Campana, Y.M.P., San Gabriel, B. and Montañez, J.J.F. (2024) 'Near field communication-triggered wireless local area network authentication', *Int. J. Internet Protocol Technology*, Vol. 17, No. 1, pp.42–52.

Biographical notes: Vincent R. Sarmiento is an Electronics Engineering student at Bicol State College of Applied Sciences and Technology (BISCAST). In his senior year, he also serves as the Vice President for External Affairs of the Institute of Electronics Engineers of the Philippines (IECEP)-BISCAST Student Chapter's Executive Committee. He has served as the Publications and Logistics Committee Head of the IECEP-Bicol Student Chapter during his junior year. His research interests include the software aspect of electronics, wireless technologies and networking.

Yna Maxene P. Campana is a fourth year Bachelor of Science in Electronics Engineering student at Bicol State College of Applied Sciences and Technology (BISCAST) and a Member of the Executive Committee of the Institute of Electronics Engineers of the Philippines-BISCAST Student Chapter. Her research interests include integrated circuit design, wireless communications, and emerging technologies such as quantum communications.

Benedick San Gabriel is a fourth year taking a Bachelor of Science in Electronics Engineering at the Bicol State College of Applied Sciences and Technology (BISCAST). He is one of the Executive Members of the Institute of Electronics Engineers of the Philippines (IECEP)-BISCAST Student Chapter, specifically the Public Relations Officer. He took up training within the Civil Aviation Authority of the Philippines for the internship course. The training taken within the transportation sector gave insights into the field, particularly communication and electronics. He gives an extent of comprehension of computer architecture and network design.

John Joshua F. Montañez obtained his Bachelor of Science in Electronics Engineering degree from the Ateneo de Naga University cum laude. He finished his Master of Engineering degree from the Bicol State College of Applied Sciences and Technology (BISCAST), where he is also a Faculty Member of the Electronics Engineering Department of the College of Engineering (CEng). He is a student of the Straight Masters-Doctorate in Electronics Engineering at the Batangas State University, the National Engineering University. Currently, he is designated as the Intellectual Property Unit Manager and the CEng Research Coordinator. His research interests are electronics engineering, artificial intelligence, engineering education and intellectual property management.

1 Introduction

In this information age, almost anyone can access data and knowledge at their fingertips. By that, it is only a matter of self-direction and discipline to be capable of almost any skill, given that one click is all it takes for a person to access an index of data he/she wishes to learn. This has dramatically impacted society in almost every aspect. However, one sector has been greatly affected by the change: education. Studies suggest (Kofo et al., 2022; O'Brien et al., 2022) that students given reliable online learning resources are more motivated and encouraged to perform better in their scholarly works. That is, especially during on-campus learning, where the environment is specialised for a conducive learning experience, a complementary provision to the students by providing access to online resources helps facilitate more effective learning. A paper on the educational experiences of Generation Z (Gen Z) students (Hernandez-de-Menendez et al., 2020) has it that they are the main contributors to a 'knowledge society' brought upon by the idea that this digitally native generation is exposed to an overwhelmingly large amount of free information which results in the acquisition of a wide array of skills. This emphasises how significant access to information, or the Internet, plays a significant role in Gen Z students' learning.

The implementation of university on-campus Wi-Fi has become prevalent due to the Internet gradually becoming a necessity for everyone, especially from an educational point of view. While this may sound like good news, campus Wi-Fi is indeed a reliable and functioning one, but it is the user login interface that creates a limiting factor and also the reason why this supposedly free Wi-Fi access is not accessible to all students by the mere fact that there is no proper account creation protocol by the institution worsen by the idea that students' database is not yet fully digitalised or if yes, does not have a well-designed network system of the digital database. Such institutional networks add a layer to the user login interface, the Captive Portal Authentication (CPA) function, a more secure and organised approach to handling organisational networks by requiring the organisation's members to authenticate via account creation to acquire access. This is a common practice for such networks, especially with the likes of school institutions (Verdadero et al., 2021). This, however, requires additional knowledge on the configuration of such authentication and frontend and backend web fundamentals.

To improve an existing and working on-campus Wi-Fi network, the researchers thought of an approach to which the additional layer brought by the Captive Portal Authentication (CPA) in the user login interface is complemented with an alternative that is more seamless while maintaining the advantages of CPA functionality. A digital communication approach, which is Near Field Communication (NFC), is seamless and a cheap digital identifier suitable for the use of an organisational network with a significantly large number of users. NFC is an emerging technology capable of high-speed communication at close range. It is an extension to the already widely used Radio Frequency Identification (RFID) technology, which only differs in the communication protocol used (Kulkarni, 2021)

The primary mechanism of the initial plan at which the entire system shall function is that the researchers shall have the main objective in the end to utilise the already existing campus wireless network of the researchers' college, Bicol State College of Applied Sciences and Technology (BISCAST), with CPA implementation, and complement the working network system with an NFC-based end-user login interface to which this shall comprise of the (1) already functioning frontend BISCAST Campus Wi-Fi software by the IT department, (2) the backend software developed by the researchers implementing NFC protocol and (3) the hardware component which comprises of the passive device providing each user a unique digital identifier and the active device in charge of linking the complementary login interface to the original login interface of CPA. The supposedly Captive Portal Authentication layer of the network to be used in the study will, however, be substituted with a more straightforward approach of using WPA/WPA2 Enterprise

authentication for convenience of conducting the study as access to the actual campus Wi-Fi where users have dedicated login credentials will first be recreated in a small scale. The WPA/WPA2 Enterprise authentication does the same function.

The study aims to create a more seamless authentication for convenience by utilising Near Field Communication (NFC) technology. This method enhances user experience by providing a seamless and efficient authentication process. Additionally, the implementation of such technology introduces new opportunities for centralised student identification and a more digitised approach to doing campus transactions, such as in library logs and accounting. The study intends to improve transaction processes in a campus-wide context, though more specifically, this study inclines more on the seamless Wi-Fi authentication method. The study is limited to using a WPA/WPA2 Enterprise authentication for the credential-based Wi-Fi login and the RADIUS server to manage the account database for user authentication.

2 Review of related literature

2.1 Emerging wireless technologies

The rise of technology is becoming completely evident nowadays, wherein wireless technology is essential in daily life. Among the cutting-edge developments in this field is the Internet of Things (IoT). The IoT concept extends internet connectivity beyond traditional devices like computers and smartphones to many other objects. This means that everything from household appliances to industrial machines can be equipped with sensors and software to collect and exchange data via the Internet. Often dubbed the 'Internet of Everything', IoT represents a significant leap towards a more interconnected world. The core of IoT systems lies in devices that gather information and transmit it over the Internet, creating a network of intelligent, connected objects. These devices communicate wirelessly, forming an intricate web of interactions that facilitate automation, improve efficiency, and enhance user experiences in numerous sectors, from smart homes to healthcare. As IoT technology continues to evolve and proliferate, its applications are becoming increasingly integral to modern life, driving forward the seamless integration of the digital and physical worlds (Mollah et al., 2019).

Another wireless technology that has become used in the modern environment is Radio Frequency Identification (RFID). RFID sensors, which combine Wireless Information and Power Transfer (WIPT), object identification and energy-efficient sensing, are revolutionising future information systems. These advanced sensors can wirelessly receive both data and power, eliminating the need for traditional power sources and enhancing sustainability. They offer precise object tracking, which is essential for applications like inventory management and logistics. At the same time, their energy-efficient design supports large-scale, long-term deployments in fields such as environmental monitoring and healthcare. By integrating these capabilities, RFID sensors provide a versatile, robust solution for modern sensing and communication needs, paving the way for more interconnected and intelligent systems (Cui et al., 2019).

Radio Frequency Identification (RFID) is essential to the Internet of Things (IoT), offering a robust solution for identifying and tracking items. This technology is extensively used across various domains, including inventory control, supply chain management, access security and asset tracking. RFID tags enable remote data capture through radio waves, allowing efficient and accurate identification without direct visual contact. This feature makes RFID a cornerstone of intelligent, interconnected systems, providing real-time information that enhances automation and operational efficiency (Zhu et al., 2019). RFID technology has rapidly expanded into diverse and complex areas, enhancing efficiency and automation across various sectors. In manufacturing and logistics, it streamlines inventory management and supply chain operations. Retail and agriculture use RFID to track and identify products, ensuring quality and safety. Toll collection and public transit systems benefit from RFID's ability to enable contactless payments and improve traffic flow. National IDs and passports with RFID chips enhance security and expedite border processing. RFID tracks medical equipment and patient information in healthcare, while pharmaceutical systems use it to prevent counterfeiting. Additionally, agriculture and food industries employ RFID to monitor livestock and manage perishable goods, reducing waste and ensuring freshness. This technology's versatility and reliability continue to drive its widespread adoption (Cui et al., 2019; Tiplea et al., 2021).

Masyuk's research delves into the intricate classification of RFID technologies based on carrier frequency, emphasising how this factor shapes their physical characteristics, operational efficiencies and constraints such as data transfer speeds and maximum transmission distances. The study highlights Near Field Communication (NFC) as a noteworthy subset within the HF frequency range of RFID technologies. Unlike conventional RFID systems, NFC devices possess the remarkable ability to function interchangeably as both readers and tags simultaneously. This unique dual-role capability has propelled NFC into the forefront of various applications, particularly in mobile technology, where it facilitates seamless communication between devices and enables innovative functionalities such as contactless payments and data exchange. Moreover, the versatility of NFC has extended its reach into diverse fields, including healthcare, where it enables the integration of intelligent functionalities into medical implants, paving the way for enhanced patient care and monitoring (Masyuk, 2019).

Furthermore, the study of Nkalo et al. (2019) illustrated how RFID technology can revolutionise student attendance management systems. By integrating RFID tags with swipe functionality and connecting them to a reader interfaced with a microcontroller-based embedded system, the researchers developed an efficient solution for monitoring student attendance. When registered students swipe their RFID tag near the reader, the system grants them entry and automatically records their attendance information in a centralised PC database. Moreover, the system provides a

failsafe mechanism: it sends an SMS to registered mobile phones, ensuring that attendance data is backed up securely and can be accessed remotely. This comprehensive approach simplifies the attendance tracking process for educational institutions and enhances data accuracy and reliability. By leveraging mobile technology, the system offers flexibility and convenience, enabling stakeholders to access attendance information anytime, anywhere, facilitating better decision-making and improving overall efficiency in academic institutions.

2.2 Near field communication

Near-Field Communication (NFC) technology has become ubiquitous in modern smart devices, offering a cost-effective wireless communication solution. Its emergence in recent years has revolutionised various aspects of daily life, including healthcare, food quality monitoring, commerce, consumer electronics and public transportation payment systems. NFC facilitates seamless interactions between devices nearby, enabling quick and convenient transactions and data exchange. Its versatility and ease of use have made it an integral part of many applications, enhancing convenience and efficiency in numerous sectors (Cao et al., 2019; Chandrasekar and Dutta, 2020). The fusion of NFC devices and sensors holds immense potential for real-world applications by introducing innovative capabilities such as wireless signal transmission and sensor functionality. This combination enables sensors to operate without external power sources while wirelessly transmitting data. Moreover, NFC devices equipped with sensing capabilities empower them to gather and process information from their surroundings, facilitating various applications across various industries. This synergy between NFC and sensors opens up exciting possibilities for enhancing efficiency, automation and convenience in everyday tasks and specialised domains (Cao et al., 2019).

NFC, an extension of RFID, is utilised for tap-and-connect functionality. When interacting with NFC devices, consumers typically engage by tapping or touching them, initiating a range of functionalities. Beyond simply reading and writing unique identification codes akin to RFID technology, NFC offers the ability to exchange diverse data types between compatible apps. This means that NFC-enabled gadgets can facilitate seamless communication and transmission of various types of content, enhancing user experiences and enabling innovative applications. Whether transferring payment information, sharing multimedia content or accessing specific functionalities within apps, NFC technology provides a convenient and versatile means of interaction for consumers across different contexts (Chandrasekar and Dutta, 2020). Near-field communication emerged nearly two decades ago as a high-security, wireless, short-range data exchange technology, such that its ability to transfer power and data between devices at the same time opens up exciting possibilities for the design of miniature, battery-free and disposable sensing systems in various everyday applications (Olenik et al., 2021).

A Near-Field Communication (NFC) tag is a compact device containing miniature microchips that store data, often a sticker or wristband. These microchips hold information that can be easily accessed by nearby mobile devices equipped with NFC technology. This enables the NFC tag to seamlessly share data with other NFC-enabled smartphones, facilitating quick and convenient interactions between devices. Whether transferring contact information, sharing digital content or initiating actions within apps, NFC tags are a convenient and versatile tool for enabling seamless communication and interaction in various scenarios (Chandrashekar and Ramamoorthy, 2023). Moreover, such devices can be used to communicate with other devices easily.

2.3 Wi-Fi as access to the internet

As technology advances into the digital age, Wi-Fi has become necessary in everyone's day-to-day life to access the internet. The research of Pahlavan and Krishnamurthy (2020) highlighted the staggering scale of connectivity facilitated by Wi-Fi access points, linking nearly one hundred billion IoT devices worldwide. These devices span a diverse range, including smartphones, tablets, laptops, smart TVs and more. This expansive network infrastructure enables seamless access to millions of applications, enhancing convenience and accessibility for users across the globe. By leveraging Wi-Fi connectivity, these devices can communicate, share data and access online services, contributing to the interconnectedness of modern digital ecosystems and enriching people's lives through enhanced connectivity and access to digital resources.

In connection, the internet can be accessed anywhere, so most people benefit from it, corresponding to their means. Nowadays, most people access the internet for their own purposes, and an example of this would be educational purposes. The study of Amponsah et al. (2022) underscored the impact of internet availability on academic performance, revealing that students with internet access tend to excel academically compared to those without. This suggests that internet accessibility plays a crucial role in shaping educational outcomes. Ghoshal and Upadhyay (2023) further elaborated on the significance of internet access for students, emphasising its role in providing unparalleled access to diverse information resources. Through the Internet, students can research, access educational materials, explore scholarly publications and gain exposure to various perspectives, enriching their learning experiences and expanding their knowledge base. This accessibility to information empowers students to deepen their understanding of subjects and fosters intellectual growth, ultimately contributing to improved academic standards and educational outcomes.

Internet access is utilised by the public nowadays, thus making it available for everyone. Since internet access has become necessary, especially for educational purposes, most schools and universities provide public internet access through wireless access points such as Wi-Fi. Captive portals are frequently employed in public internet access settings, requiring users to enter a username and password for authentication. However, this method is often viewed as vulnerable to security breaches, as intruders can access others' accounts. In response to this concern, a study implemented RFID technology to authenticate students' internet credentials through captive portals (Grancho et al.,

2021). By leveraging RFID, students could securely validate their identity without relying solely on usernames and passwords. This approach enhances security and mitigates the risk of unauthorised access, thereby improving the overall integrity of the internet access system in educational environments.

2.4 Near field communication as an interfacing method

With the rise of NFC technology in recent years, it is mainly used in various day-to-day applications. Incorporating NFC into cell phones has enabled a wide range of applications. In Ali et al. (2020), NFC-Stego, a cutting-edge data concealment technique, was introduced. This innovative mechanism leverages the secure connection between NFC-enabled Android smartphones to effectively hide large volumes of data. NFC-Stego offers robust security measures while maintaining user-friendly operation, making it a practical solution for concealing sensitive information. Utilising NFC technology ensures imperceptibility while enhancing data security, thus addressing the need for secure data transmission and storage in mobile environments.

The study of Chiang et al. (2022) demonstrated the practical application of GPS and NFC technologies in creating an attendance tracking system. By leveraging these technologies, mainly on Android smartphones, the system offers a reliable method for managing student attendance. GPS enables accurate location tracking, while NFC facilitates seamless interaction with attendance checkpoints or tags. Combining these technologies provides an efficient and automated solution for tracking student attendance, improving accuracy and reducing administrative burden. This innovative approach demonstrates the potential of leveraging smartphone capabilities to enhance traditional attendance management processes in educational settings.

Tafti et al. (2021) presented a novel NFC mobile payment protocol designed to enhance security in mobile payment transactions. This protocol addresses vulnerabilities in Global System for Mobile (GSM) authentication by employing asymmetric encryption for mutual authentication, reducing the risk associated with symmetric cryptographic methods. By minimising the required key pairs and implementing advanced security measures, such as protection against replay attacks, Denial-of-Service (DoS) attacks, eavesdropping, repudiation, man-in-the-middle attacks and desynchronisation, the protocol enhances the overall resilience of mobile payment systems. Furthermore, the protocol is tailored to the limitations of mobile devices by reducing client-side signalling overhead and processing load, ensuring efficient and secure payment transactions while leveraging NFC technology.

One of the problems encountered with Near Field Communication devices is security authentication. Lu and Liu (2021) introduced an enhanced NFC device authentication protocol that effectively safeguards against various security threats. This protocol demonstrates resilience against brute force attacks, man-in-the-middle attacks and replay attacks, ensuring the integrity of the authentication process. Moreover, it streamlines message transmissions, enhancing transmission efficiency while bolstering the confidentiality, integrity, non-repudiation and overall security of NFC device authentication. The protocol offers a robust and reliable solution for ensuring secure interactions between NFC-enabled devices by addressing these security concerns and optimising authentication procedures.

2.5 Similar studies

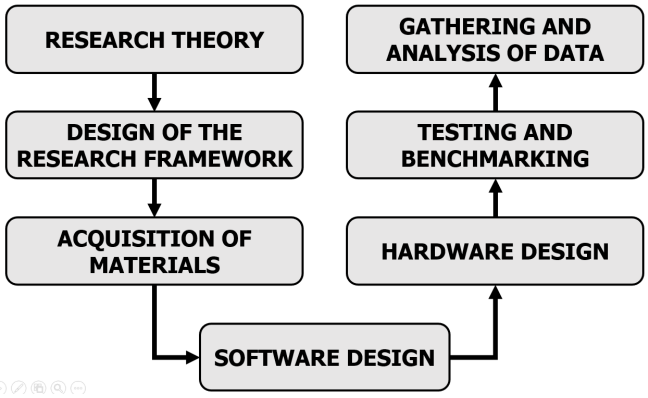
The concept of user login interfaces, as highlighted in Hernandez-de-Menendez et al. (2020) and Grancho et al. (2021), underscores the importance of captive portals in facilitating internet access, particularly within campus Wi-Fi networks. These portals serve as gateways for users to authenticate their identities and gain access to the Internet securely. Additionally, Chiang et al. (2022); Tafti et al. (2021); Brumerčíková and Buková (2020) and Platov et al. (2021) shed light on the versatile applications of NFC technology beyond internet access. From electronic wallets to attendance tracking systems and tourism-related applications, NFC technology offers various functionalities that enhance convenience and efficiency in various domains. These studies showcase how NFC technology can be leveraged to streamline processes, improve security and enrich user experiences in different contexts.

In summary, these related studies correlate to the researchers' study, which mainly focuses on utilising near-field communication along with Captive Portal Authentication to access campus wireless networks with ensured security and seamless transactions among end-users at the chosen campus, Bicol State College of Applied Sciences and Technology (BISCAST).

3 Methodology

A systematic approach to the study's progressive completion sequence is necessary for its success. This section of the paper shall cover how the research study was conducted sequentially. The paradigm of the study is expressed in the preceding Figure 1.

Figure 1 Paradigm of the study



3.1 Research theory

The foundations of this research study shall be based on the existing theories about Near Field Communication and its possible applications. Also, with emphasis on its application in seamless transactions, the research theories included here encompass support on the how's and whys of NFC as a user interface function for a particular digital process, which, in the case of this study, is the connection to a wireless access point. To elaborate on each theoretical knowledge involved:

- *Near-field communication*: Also known as NFC, this technology was developed for short-range radio communication (Betion, 2022). It has seen various applications in different sectors of society, such as transportation or restaurant payment systems (Srun et al., 2023; Yu and Fang, 2023). The contactless triggering appeal when it is used is among the features that will be implemented in this study.
- *Captive portal authentication*: A captive webpage portal where users are redirected for authentication (Asplund, 2021).
- *Remote authentication dial-in user service*: A networking protocol that authorises and authenticates users who access a remote network (Kizza, 2024; Yudhistira and Harwahyu, 2024).

3.2 Acquisition of materials

Particular materials are needed to create the specific processes necessary for the study. NFC tags and the NFC Read/Writer create the NFC protocol. The researchers will use a wireless access point and computer to build a foundational backend design. The materials prerequisites to conducting the study are listed below in Table 1.

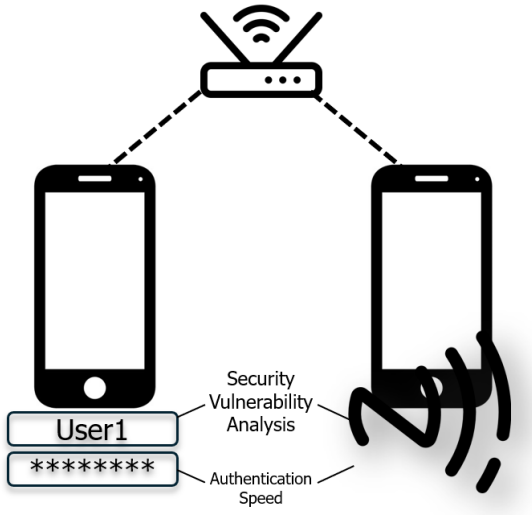
Table 1 List of materials

Material	*Quantity*
Computer	1
NFC Tags (NTAG215)	200
Wireless Router with RADIUS capability	1
NFC-capable Mobile Phone	1

3.3 Design of the research framework

The study's end product is expected to provide a service in the form of improved ease of access to the campus Wi-Fi for the end-users, students and faculty of BISCAST. This shall be made possible through the utilisation of a software and hardware mechanism. The design of this mechanism revolves around the use of Near-Field Communication (NFC) as a medium of authentication in connecting the Wi-Fi network.

Figure 2 Framework of the study



3.4 Software design

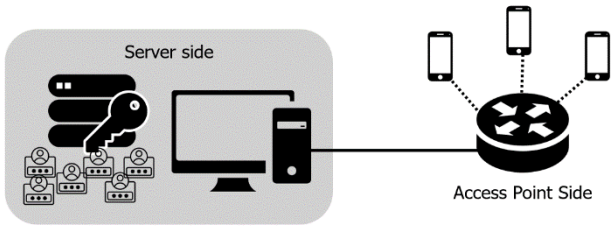
The software design of the system will play the most significant role in the mechanism of NFC as a medium to authenticate a Wi-Fi connection with a mobile device. The authentication pertained in the study means using already existing authentication protocols such as WPA/WPA2 Pre-Shared and WPA/WPA2 Enterprise. NFC will solely be the medium at which the authentication protocol is to be communicated.

- *Network Setup*: The need for an authentication protocol arises from technological advancements in communicating various information. We have adapted these modern communication methods to our daily lives, from which sensitive information may be prone to mal-intended users. Authentication is part of a more extensive communication protocol to authenticate and grant access to the communication. To establish this connection between two nodes, a network must first be set up. To begin with, the researchers created a system for an NFC as a medium for authenticating Wi-Fi connection, and a small network was created to connect a few mobile devices wirelessly. Wireless routers served as the access point altogether in the study, and the choice of device that was considered to be used in the study was the one that was capable of a connection with the RADIUS server.
- *Database Setup*: Remote Authentication Dial-in User Service (RADIUS) will be the backbone of the database and security of the system. RADIUS is responsible for the authentication in a specific case of wireless network authentication setup: WPA/WPA2/WPA3 Enterprise, where a dedicated credential is allotted to one device at a time. This setup of wireless LAN connectivity was used together for its suitability for an institutional network needing one account for each user to connect with.

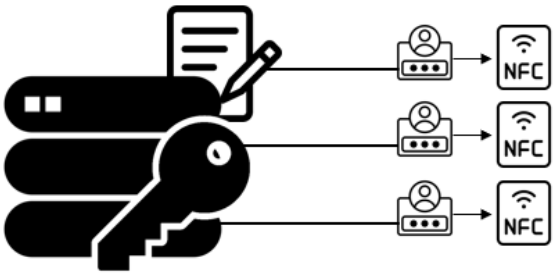
- *Account assignment to NFC tags*: A network setup with a RADIUS Server for the account database and authentication is already functioning and robust. Through this setup, user identities or the username and password for each account are needed to establish a Wi-Fi connection.

The system's software mechanism comprises the network setup for a functioning access point connected to the RADIUS server and the writing of credentials to the NFCs. Figure 3(a) shows that the access point is connected to the database server, which is the RADIUS, wherein once a user requests authentication for access from the access point, it verifies with the accounts listed on the server side after accounts with its dedicated credentials were created. Figure 3(b) shows that account creation must first be conducted in the database server, followed by the NFC writer to input the account's credentials into its assigned NFC.

Figure 3 Software mechanism of the system (a) For the network setup configured with remote authentication dial-in user service server and (b) Implementation of Wi-Fi login credentials through an NFC-read/writer



(a)

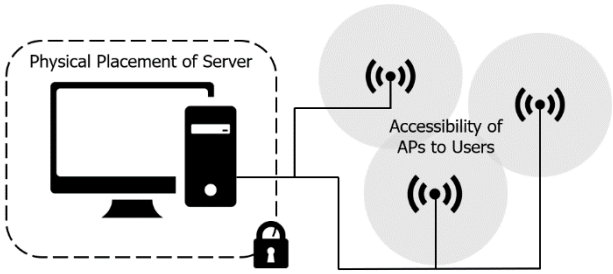


(b)

3.5 Hardware design

The hardware setup of the system will be minimal as only the software part is where the central mechanism will be based. One primary consideration in defining the hardware setup would be the secure positional placement of the server Computer and router to avoid possible unauthorised access to the database of user credentials. Positioning of access points should also be considered, as this may affect the speed of establishing a connection with the wireless network. Designing the hardware setup will follow the specific network topology setup. On the user side, user-specific tags will be integrated with the BISCAST student ID, which opens up possible paths toward digitalised student-centred services or protocols like attendance recording and a library log. Figure 4 shows the physical network topology. It highlights the need for a secure server placement away from any physical disruptions affecting its performance and the optimal placement of multiple access points for accessible signal strength.

Figure 4 Simplified physical network topology



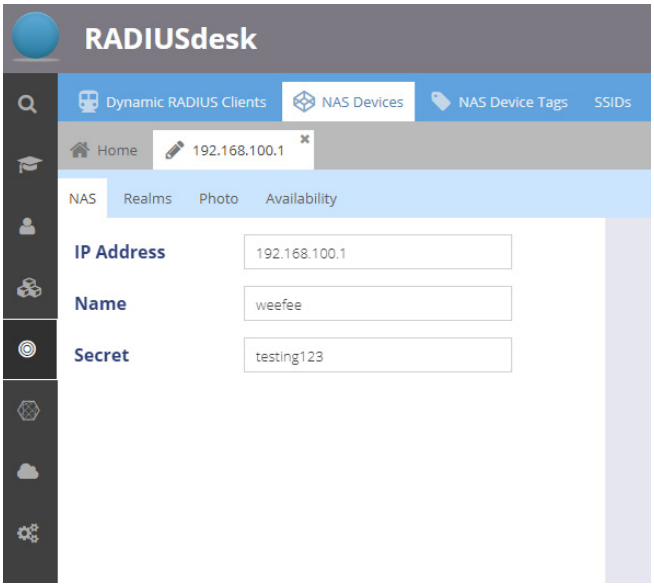
3.6 Testing/benchmarking

In testing and benchmarking the NFC-triggered Wi-F connection, the main parameter to be tested is the speed or responsiveness of the proposed method. Several tests will be conducted as well as the other constant variables that may affect the testing if not careful, which may include distance from the access point, the access point to be connected to among all tests must be and have the same configuration, and the specific type of NFC tag used as well as the manner of tapping the NFC-tag to the mobile device which is specified and limited only to an android mobile phone capable of NFC communication. All trials conducted in the test have constant distance from the access point, indicating the highest signal strength level without obstruction between the mobile phone and the access point. The access point and set up to be used at which the mobile phone will establish its connection are similar throughout the test, explicitly using the Huawei EchoLife EG8245h5 router. Speed and responsiveness will be measured through the time difference between the moment of tapping the NFC tag on the mobile device and the time the connection was established with the wireless network. For the traditional method, the authentication speed will be measured from when the user begins inputting its credentials until the connection is established with the wireless network. Manual speed measurement was conducted through a digital stopwatch, accounting for human error minimised to ±0.5 s.

In the security vulnerability aspect, observation will be made based on the qualities and conditions at which such vulnerabilities are possible. The passwords used throughout the test are similar to each 8-character, 16-character and 24-character password composed of a combination of alphanumeric and special characters. Password length begins with eight characters per NIST SP800-63B recommendations on digital identity guidelines to be relatively strong. The results of the test and observation shall be recorded for further analysis.

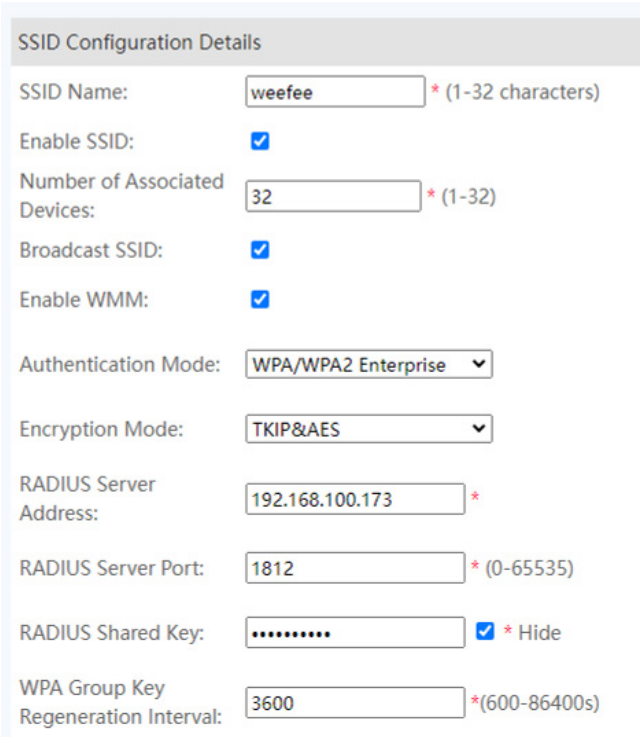
The RADIUS server was created using RADIUSdesk, an open-source authorisation, authentication and accounting implementation in a network setup, as seen in Figure 5. The software was installed on a computer device and set up through the server's configuration page. To establish a connection with the router capable of RADIUS, the IP address, SSID and the RADIUS shared key were configured.

Figure 5 RADIUS server setup of router connectivity (see online version for colours)



Once the RADIUS Server was done with the setup, its connectivity to the router was established through the router's configuration page, as shown in Figure 6. The figure shows the WLAN's configuration, specifically on a Huawei EG8245H5 router. The authentication mode was selected as WPA/WPA2 Enterprise, configured to connect with the RADIUS server address provided with the server port and the shared key for communicating the credentials database.

Figure 6 Router setup of WPA/WPA2 enterprise and RADIUS server address (see online version for colours)



After successfully establishing a connection between the RADIUS server and the router, three accounts were created. This was accessed through Figure 7, the RADIUS server's configuration page for user account creation. Credentials were of varying password lengths which are to be used in the testing.

Figure 7 Account creation in radius server (see online version for colours)

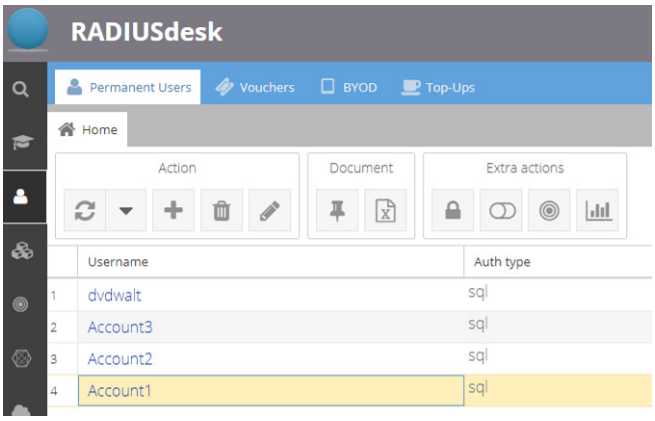
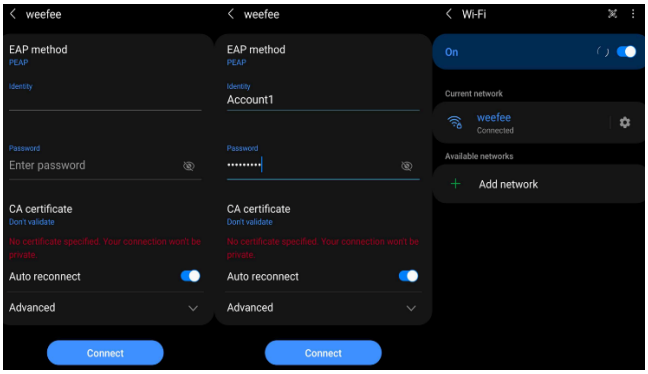


Figure 8 shows the traditional method of inputting account credentials in a WPA/WPA2 Enterprise authentication. Connectivity to the network was established after the correct account credentials were input.

Figure 8 Testing with manual account credential input (see online version for colours)



3.7 Gathering and analysis of data

Part of the study involves using necessary statistical tools to analyse how raw information gathered must be processed for a more digestible interpretation. An analysis of observable vulnerabilities was conducted using the traditional way of authenticating a Wi-Fi connection and the NFC-triggered approach. Observations are then inputted as qualitative data, which will be the basis for the interpretation of the later part of the study.

4 Results and discussion

This chapter presents the findings of the study based on the testing and simulation of the device as well as data gathered from the distributed survey forms for end-user acceptability among the respondents. This provides an analysis and

interpretation of the gathered data results based on defined parameters to measure the significance of the authentication triggering method for Wi-Fi connectivity compared to a traditional way of inputting credentials.

Security vulnerabilities are observed when we authenticate a Wi-Fi connection traditionally in which we type in the credentials compared to when we substituted this method by binding the credentials instead to an NFC tag and letting it serve as a key in which we tap to a mobile device to connect seamlessly to the Wi-Fi. From the analysis, settling for an NFC-triggered authentication solves some vulnerabilities, such as eavesdropping on credentials upon inputting and the circumstances in which we forget the password. However, this has introduced some new vulnerabilities specific to the use of NFC, such as data tampering and cloning when the NFC tag used is not locked in any way, and credentials may still be eavesdropped on.

Table 2 Security vulnerability analysis

NFC-Triggered	*Traditional*
Eavesdropping through unauthorised reading of NFC Tag	Eavesdropping of credentials, especially in crowded spaces.
Data input is seamless and requires close contact	Data input through typing adds additional risk of eavesdropping
Risk of data tampering on NFC tags	No risk of data tampering
There is no risk of forgetting complicated passwords as data is stored in the tag.	Risk of forgetting the complicated password

From Table 3, results on the speed of authentication through NFC given different password lengths have small variability, having a mean value of 9.82, which is close to the values obtained. A test of one-way analysis of variance for the data shows no significant difference in the authentication speed among three password length groups with a *p*-value of 0.799, which is much greater than the threshold of 0.05.

Table 3 Test for authentication speed results using NFC-triggered method

Length of credentials for authentication	*Speed of authentication (seconds)*			
	Trial 1	*Trial 2*	*Trial 3*	*Avg.*
8-character password	9.74	9.55	10.63	9.97
16-character password	9.63	9.38	10.22	9.74
24-character password	9.75	9.37	10.13	9.75

Table 4 shows the data gathered using the traditional method of manually typing credentials for authentication. In contrast to the NFC-triggered method, the traditional method of authentication has higher variability in terms of speed when faced with different credential lengths. There is an average increase of 9.55 seconds in authentication for every 8-character increase in the password length. A One-Way Analysis of Variance statistical test was conducted to verify the significance of the authentication speed of the three password groups. The test garnered a result of 0.0000755 p-value, which is significantly less than the 0.05 threshold, indicating a significant difference in the authentication speed among the three password length groups.

Table 4 Test for authentication speed results using the traditional method

Length of credentials for authentication	*Speed of authentication (seconds)*			
	Trial 1	Trial 2	Trial 3	Avg
8-character password	20.87	17.92	19.71	19.5
16-character password	26.83	32.46	29.88	29.72
24-character password	39.24	39.56	37.00	38.6

Authentication speed was tested using the NFC-triggered method, and the traditional method was tested using various credentials for authenticating. This parameter was considered in the testing to determine whether it may affect the authentication time. Upon checking data usage of different password lengths, an eight-character difference equates to an eight-byte difference, and also, in situations where users try to input a combination of alphanumeric characters and make it long, there might be a difference in the speed of authentication.

From the results gathered, in the one utilising NFC to authenticate, the eight-byte difference of credentials does not significantly affect the speed of authentication. This data is helpful as we can infer that using a long password may be possible and practical for once. Using long or short does not significantly affect the authentication speed but does increase the security against brute force attacks due to the larger number of combinations needed with more characters. In contrast, there is a barrier to convenience for users when using long passwords through the traditional way of authenticating, which is typing the credentials. From the results on authentication speed results when typing such credentials, using longer passwords takes a toll on users' convenience as it took longer for them to authenticate.

5 Conclusion and recommendation

The researchers' findings on the study's parameters focusing on NFC-triggered wireless LAN authentication have shown significant results upon comparing its authentication speed with the traditional manner. Also, the analysis of security vulnerabilities between the two shows a similar position when compared to each other, as introducing NFC does solve some security vulnerabilities but introduces another one. In the end, though, using NFC brings users more convenience because of the effortless authentication method and speed. In conclusion, the proposed method does meet its intended purpose of creating a more seamless and convenient authentication method. Several aspects of the study were conducted under certain limitations, which may have drastically influenced the direction of the study. These limitations include the specific use of WPA/WPA2 Enterprise Authentication utilising a

remote dial-in user service server (RADIUS) to verify and manage user access to the network, and testing was only done with an Android Phone with NFC capability. The traditional authentication method pertains to the conventional way of manually typing down credentials. Acknowledging the limitations, the results of the study are bound to such factors; thus, performing under different setups like the use of Captive Portal Authentication rather than the used WPA/WPA2 Enterprise would have a general effect on the results of the study as it would require a router capable of captive portal or another device server which would authenticate the captive portal connections and store user database. The study aims to provide faster, seamless and minimise the security risks from the traditional way of manually inputting user credentials to connect to a network.

Further improvements may be made in the security aspect of the study, wherein WPA/WPA2 Enterprise has weaknesses. The security in the RADIUS server must be largely emphasised as this holds the user credentials covering all the sensitive data for users to access the network. Similarly, on the user side of the network, unauthorised access may still be possible once the user's credentials are compromised; hence, a multi-factor authentication procedure may be deemed necessary. The multi-factor authentication is to be communicated with the RADIUS server's backend, adding another layer of security to the network.

Acknowledgement

The researchers would like to express their gratitude to the Bicol State College of Applied Sciences and Technology for its support in completing this paper.

References

Ali, A.A., Saad, A-H.S. and Ismael, A.H. (2020) 'Data hiding technique based on NFC-enabled smartphones', *Procedia Computer Science*, Vol. 171, pp.2400–2409. Doi: 10.1016/j.procs.2020.04.260.

Amponsah, K.D., Aboagye, G.K., Narh-Kert, M., Commey-Mintah, P. and Boateng, F.K. (2022) 'The impact of Internet usage on students' success in selected senior high schools in Cape Coast metropolis, Ghana', *European Journal of Educational Sciences (Kočani)*, Vol. 9, No. 2, pp.1–18. Doi: 10.19044/ejes.v9no2a1.

Asplund, T. (2021) *Design and Implementation of a Wi-Fi Portal System*, Abo Akademi University. Available online at: https://urn.fi/URN:NBN:fi-fe2021060835660 (accessed on 2 April 2024).

Betion, H.J. (2022) 'Near field communication', *A student presentation to the Fall 2022 Student Research and Creative Works Symposium*. Available online at: http://hdl.handle.net/10790/7141 (accessed on 2 April 2024).

Brumerčíková, E. and Buková, B. (2020) 'Proposals for using the NFC technology in regional passenger transport in the Slovak Republic', *Open Engineering (Warsaw)*, Vol. 10, No. 1, pp.238–244. Doi: 10.1515/eng-2020-0005.

Cao, Z., Chen, P., Ma, Z., Li, S., Gao, X., Wu, R., Pan, L. and Shi, Y. (2019) 'Near-field communication sensors', *Sensors (Basel)*, Vol. 19, No. 18. Doi: 10.3390/s19183947.

Chandrasekar, P. and Dutta, A. (2020) 'Recent developments in near field communication: A study', *Wireless Personal Communications*, Vol. 116, No. 4, pp.2913–2932. Doi: 10.1007/s11277-020-07827-9.

Chandrashekar, L. and Ramamoorthy, L. (2023) 'Use of near field communication (NFC) tags in dermatology', *Indian Dermatology Online Journal*, Vol. 14, No. 1, p. 138. Doi: 10.4103/idoj.idoj_205_22.

Chiang, T-W., Yang, C-Y., Chiou, G-J., Lin, F.Y-S., Lin, Y-N., Shen, V.R.L., Juang, T.T-Y. and Lin, C-Y. (2022) 'Development and evaluation of an attendance tracking system using smartphones with GPS and NFC', *Applied Artificial Intelligence*, Vol. 36, No. 1. Doi: 10.1080/08839514.2022.2083796.

Cui, L., Zhang, Z., Gao, N., Meng, Z. and Zhen, L. (2019) 'Radio frequency identification and sensing techniques and their applications – a review of the state-of-the-art', *Sensors*, Vol. 19, No. 18. Doi: 10.3390/s19184012.

Ghoshal, S. and Upadhyay, A. (2023) 'The effect of Internet on students' studies – a review', *EPRA International Journal of Multidisciplinary Research (IJMR)*, Vol. 9, No. 7, pp.38–42. Available online at: https://eprajournals.com/IJMR/article/10931/abstract (accessed on 1 April 2024).

Grancho, D.P., Talirongan, F.J.B. and Talirongan, H. (2021) 'Security measures implementation on the web access: university's turnstile interfacing', *Mediterranean Journal of Basic and Applied Sciences*, Vol. 5, No. 1, pp.28–39. Doi: 10.46382/MJBAS.2021.5103.

Hernandez-de-Menendez, M., Escobar Diaz, C. and Morales-Mendez, R. (2020) 'Educational experiences with Gen Z', *International Journal on Interactive Design and Manufacturing (IJIDeM)*, Vol. 14, No. 4, pp.847–859. Available online at: https://link.springer.com/article/10.1007/s12008-020-00674-9 (accessed on 2 April 2024).

Kizza, J.M. (2024) *Authentication: in Guide to Computer Network Security*, Springer International Publishing, Cham, pp.215–238. Doi: 10.1007/978-3-031-47549-8_10.

Kofo, S.A., Ochayi, O.A. and Jimoh, B.A. (2022) 'Access and utilization of online learning resources among undergraduate students', *Indonesian Journal of Educational Research and Review*, Vol. 5, No. 1. Available online at: https://ejournal.undiksha.ac.id/index.php/IJERR/article/view/45959 (accessed on 1 April 2024).

Kulkarni, R.D. (2021) 'Near field communication (NFC) technology and its application', *Techno Societal 2020*, pp.745–751. Doi: 10.1007/978-3-030-69921-5_74.

Lu, H-J. and Liu, D. (2021) 'An improved NFC device authentication protocol', *PloS One*, Vol. 16, No. 8. Doi: 10.1371/journal.pone.0256367.

Masyuk, M. (2019) 'Information security of RFID and NFC technologies', *Journal of Physics: Conference Series*, Vol. 1399, No. 3. Doi: 10.1088/1742-6596/1399/3/033093.

Mollah, M.B., Zeadally, S. and Azad, M.A.K. (2019) 'Emerging wireless technologies for internet of things applications: opportunities and challenges', *Springer eBooks*, pp.1–11. Doi: 10.1007/978-3-319-32903-1_328-1.

Nkalo, U.K., Agwu, E.O. and Stanley, E.C. (2019) 'Radio frequency identification (RFID) based attendance system with short message service (SMS) backup', *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 21, No. 2, pp.01–08. Doi: 10.9790/0661-2102010108.

O'Brien, O., Sumich, A., Kanjo, E. and Kuss, D. (2022) 'Wi-Fi at university: A better balance between educational activity and distraction activity needed', *Computers and Education Open*, Vol. 3. Doi: 10.1016/j.caeo.2021.100071.

Olenik, S., Lee, H.S. and Güder, F. (2021) 'The future of near-field communication-based wireless sensing', *Nature Reviews. Materials*, Vol. 6, No. 4, pp.286–288. Doi: 10.1038/s41578-021-00299-8.

Pahlavan, K. and Krishnamurthy, P. (2020) 'Evolution and impact of Wi-Fi technology and applications: a historical perspective', *International Journal of Wireless Information Networks*, Vol. 28, No. 1, pp.3–19. Doi: 10.1007/s10776-020-00501-8.

Platov, A.V., Tarchokov, S.K., Zikirova, Sh., Litvinova, O.I. and Udalov, D.E. (2021) 'NFC technology acceptance factors in tourism', *DEFIN-2021: IV International Scientific and Practical Conference*. Doi: 10.1145/3487757.3490928.

Srun, C., et al. (2023) 'Design of a bus payment system using near-field communication (NFC)', *Proceedings of the International Conference on Advanced Mechatronics, Intelligent Manufacture and Industrial Automation (ICAMIMIA)*. Doi: 10.1109/ICAMIMIA60881.2023.10427961.

Tafti, F.S.M., Mohammadi, S. and Babagoli, M. (2021) 'A new NFC mobile payment protocol using improved GSM-based authentication', *Journal of Information Security and Applications*, Vol. 62. Doi: 10.1016/j.jisa.2021.102997.

Ţiplea, F.L., Andriesei, C. and Hristea, C. (2021) 'Security and privacy of PUF-based RFID systems', *IntechOpen eBooks*. Doi: 10.5772/intechopen.94018.

Verdadero, A.G., Villanueva, J., Llorca, A., Marfil, J. and Mendoza, A. (2021) 'Wi-Fi captive portlet implementing internet of everything for Trimex Colleges Inc.', *International Journal of Advanced Research in Computer Science*, Vol. 12, No. 4, p.38. Doi: 10.26483/ijarcs.v12i4.6755.

Yu, W.W. and Fang, C. (2023) 'Embracing sustainability: assessing the influence of near-field communication mobile payment systems on restaurant operating performance', *Preprints.org Business, Economics, and Management*. Available online at: https://www.preprints.org/manuscript/202307.0454/v1 (accessed on 2 April 2024).

Yudhistira, A.D. and Harwahyu, R. (2024) 'Implementation strategy analysis of network security using dalo RADIUS and Pi-hole DNS server to enhance computer network security: case study: XYZ as a fintech company', *Jurnal Indonesia Sosial Teknologi*, Vol. 5, No. 10, pp.4364–4379. Doi: 10.59141/jist.v5i10.5321.

Zhu, F., Li, P., Xu, H. and Wang, R. (2019) 'A lightweight RFID mutual authentication protocol with PUF', *Sensors (Basel)*, Vol. 19, No. 13. Doi: 10.3390%2Fs19132957.