International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Devoloping a Two Factor Authentication System to Identify Vulnerabitlies in Public Wifi Leading to Hovac Attacks

Israa Ahmed Jaddoa JADDOA1,
Asst.Prof.Dr. Ayca Turkben Kurnaz2
1,2 Information Technologies, Altinbas university, Istanbul, Turkey.
israa198653@gmail.com1, ayca.kurnaz@altinbas.edu.tr 2

Abstract

Although public Wi-Fi networks offer a lot of convenience, users should be aware that their data may not always be safe. Hackers are able to launch cyber-attacks by taking advantage of vulnerabilities in these networks. These attacks include the so-called HOVAC attacks, which stand for hacktivism, organized crime, vendetta, espionage, and cyber warfare. We propose a two-factor authentication system that identifies vulnerabilities in public Wi-Fi networks as a means of reducing the likelihood that such attacks would be successful. A way for authenticating users via passwords serves as the initial component in our multi-factor authentication system. In order for users to connect to a public Wi-Fi network, they will be required to enter a password. This password will be one of a kind for each individual user, and it will be kept in a protected database. Before a user is allowed to connect their device to the network, our authentication system will conduct a vulnerability scan on the user's device as the second factor in the authentication process. This scan will determine whether or not the user's device contains any vulnerabilities that a hacker might be able to take advantage of. Before the user is allowed to connect to the network, they will be urged to take action to remedy any vulnerabilities that may have been discovered during the scan. In order to create this system, we will employ a variety of different methods, including data analysis and machine learning. We are going to collect data on public Wi-Fi networks and then apply machine learning techniques in order to detect patterns of vulnerabilities that are frequently exploited by hackers. We will also conduct an analysis of data pertaining to HOVAC assaults in order to determine the commonalities shared by these attacks, such as the different sorts of vulnerabilities that are exploited. When we have completed development of the authentication system, we will put it through its paces in an environment more representative of the actual world in order to determine how well it performs. We will collaborate with companies who supply public Wi-Fi to install the technology on their networks and monitor how well it operates over time. In addition, we will solicit input from users in order to ascertain whether or not they have any problems or worries regarding the system. In short, the proposed two-factor authentication

system that we have developed is intended to detect flaws in public Wi-Fi networks and reduce the likelihood of HOVAC cyber assaults. We want to achieve our goal of providing customers with a method that is both secure and convenient for connecting to public Wi-Fi networks by combining password-based authentication with vulnerability scanning.

Keywords: HOVAC ,Wi-Fi, 2FA.

Introduction

The proliferation of public Wi-Fi networks in a wide variety of locations, such as airports, hotels, restaurants, and shopping malls, has made it much simpler for users to connect to the internet. Users who connect to public Wi-Fi networks, on the other hand, put themselves in a vulnerable position with regard to potential cybersecurity threats [1]. One of the most significant risks is the possibility of a hacker launching a cyberattack that can be classified as an HOVAC (hack, own, violate, attack, and compromise). This is a type of attack in which the hacker would hack, own, violate, attack, and compromise the system. Theft of personal and sensitive information, such as passwords, financial information, and even an individual's identity, can be the result of a cyberattack of this type. As a consequence of this, it is of the utmost importance to develop a trustworthy two-factor authentication system in order to identify vulnerabilities in public Wi-Fi networks and cut down on the likelihood of HOVAC attacks [1].

The widespread adoption of Wi-Fi networks and the subsequent attack by HOVAC on those networks

The growing demand for internet connectivity and the proliferation of devices that are enabled with Wi-Fi have directly led to a rapid increase in the deployment of Wi-Fi networks over the past few years. This has resulted in a rapid increase in the overall number of devices that are enabled with Wi-Fi. Wi-Fi connectivity has rapidly become an expected amenity in a wide variety of public venues, including cafes, shopping centers, airports, and hotels, amongst other public settings. On the other hand, due to an increase in the number of people using Wi-Fi networks, the possibility of cyberattacks has also grown along with it. HOVAC, which stands for "hack, own, violate, attack, and compromise," is an example of this kind of attack. HOVAC stands for "hack, own, violate, attack, and compromise." This kind of attack can result in the theft of sensitive information like passwords, financial information, and even the identity of a person [2].

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

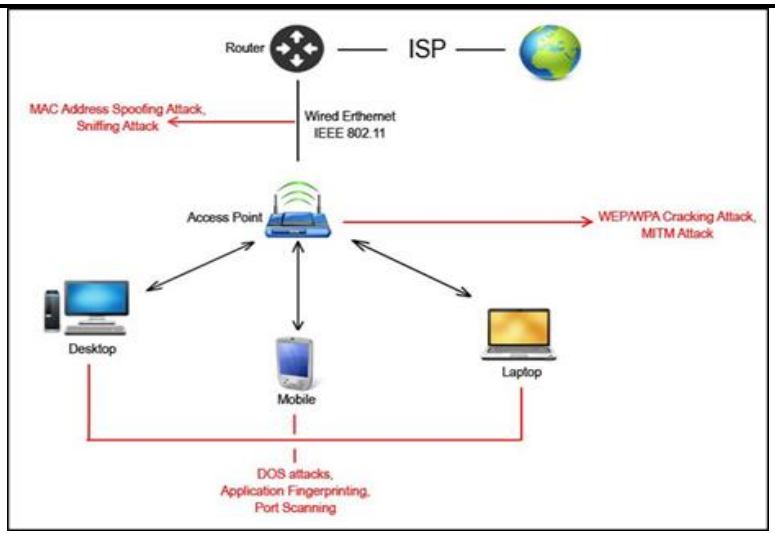

Figure **Error! No text of specified style in document.**: Router and isp reader for worldwide [2].

Expanding the capacity of existing Wi-Fi networks

The Internet of Things (IoT) has led to an increase in the distribution of Wi-Fi network infrastructure, which has resulted in the technology becoming more widespread than it ever has been before. The Internet of Things (IoT) refers to the network of devices that are able to communicate with one another in addition to their ability to communicate with the internet. This category includes a wide variety of electronic products, some examples of which include smart phones, tablets, laptop computers, smart homes, and wearable technology. In response to the ever-increasing number of devices that are being added to the Internet of Things network, there has been a meteoric rise in the demand for Wi-Fi connectivity [3]. One of the most significant benefits provided by these kinds of networks is the ability of Wi-Fi networks to simultaneously provide internet connectivity to a number of different types of devices. This is one of the most significant advantages. Because of this quality, wireless local area networks (Wi-Fi) are ideally suited for use in public places such as cafes, airports, and hotels, where a large number of users need to access the internet at the same time. Specifically, this makes Wi-Fi networks an attractive option. Wi-Fi networks also offer greater mobility than traditional wired networks do, allowing users to freely move around while still remaining connected to the network [3]. This is because Wi-Fi networks use radio waves rather than wires to transmit data. This is due to the fact that data is transmitted over Wi-Fi networks via radio waves rather than wires. On the other hand, an increase in the number of Wi-Fi networks has led to a rise in the number of potential targets for cyberattacks [4].

HOVAC Attack

HOVAC attacks are a form of cyber-attack that are designed to steal sensitive information from Wi-Fi networks [4]. These attacks are carried out by hackers. Hacker groups are responsible for carrying out these assaults. The attack can be broken down into five distinct stages, which are as follows:

i. The intruder will begin the hack by first gaining access to the Wi-Fi network without authorization in the first stage of the process. This can be accomplished through a variety of methods, such as making use of vulnerabilities in the network's security system or employing

brute-force attacks in an effort to figure out the network's passwords. Both of these methods are viable options [4].

ii. Once an adversary has successfully breached a network's defenses, they are in a position to claim ownership of the system and assume control of its operations. This entails disabling any potential security features that may be present as well as putting in place backdoors so that access can be maintained to the network [4].

iii. The adversary is now in a position to intercept and monitor the traffic that is going through the network at this stage of the process. This can include obtaining sensitive information about the individual, such as their login credentials, financial information, and personal data [4].

iv. Attack: Once the attacker has gathered all of the necessary information, they are in a position to launch targeted attacks against specific individuals or organizations. These attacks can be very damaging. Phishing and malware infections are a couple of examples of the types of attacks that can be categorized into this category [5].

v. Compromise: This is the final stage, in which the attacker can use the information that they stole to compromise the security of the network as well as the devices that are connected to it [6].

vi. In order to lessen the likelihood that HOVAC will come under attack [6]:

vii. One can reduce the likelihood of HOVAC attacks on Wi-Fi networks in a number of different ways by taking advantage of the various strategies that are available to them. One of the most effective ways to achieve this is to put stringent security measures into place. The following are some examples of possible countermeasures [6]:

viii. Encryption: It is strongly recommended that encryption be used on Wi-Fi networks, and a strong encryption standard such as WPA2 should be utilized. This results in an increase in the information's level of confidentiality as it is transmitted across the network [6].

ix. Passwords: The passwords that are utilized to gain access to Wi-Fi networks should be strong and convoluted in order to reduce the risk of unauthorized access. This defense can protect against assaults that rely on overwhelming force [6].

x. When a network employs the security measure known as "two-factor authentication," users are required to provide not one but two distinct forms of identification before being granted access to the network. It is possible that this strategy will prove to be an effective method for restricting access to the network by unauthorized users [6].

xi. The process of dividing a larger network into several smaller subnetworks is referred to as "network segmentation," and it is denoted by the term "network segmentation." This has the potential to stop the spread of malicious software and lessen the severity of the impact that attacks have [7].

xii. Monitoring: Administrators of Wi-Fi networks should be on the lookout for unusual activity and keep a close eye on the network at all times. It is possible for this to help in the early detection of attacks and the prevention of data theft [7].

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

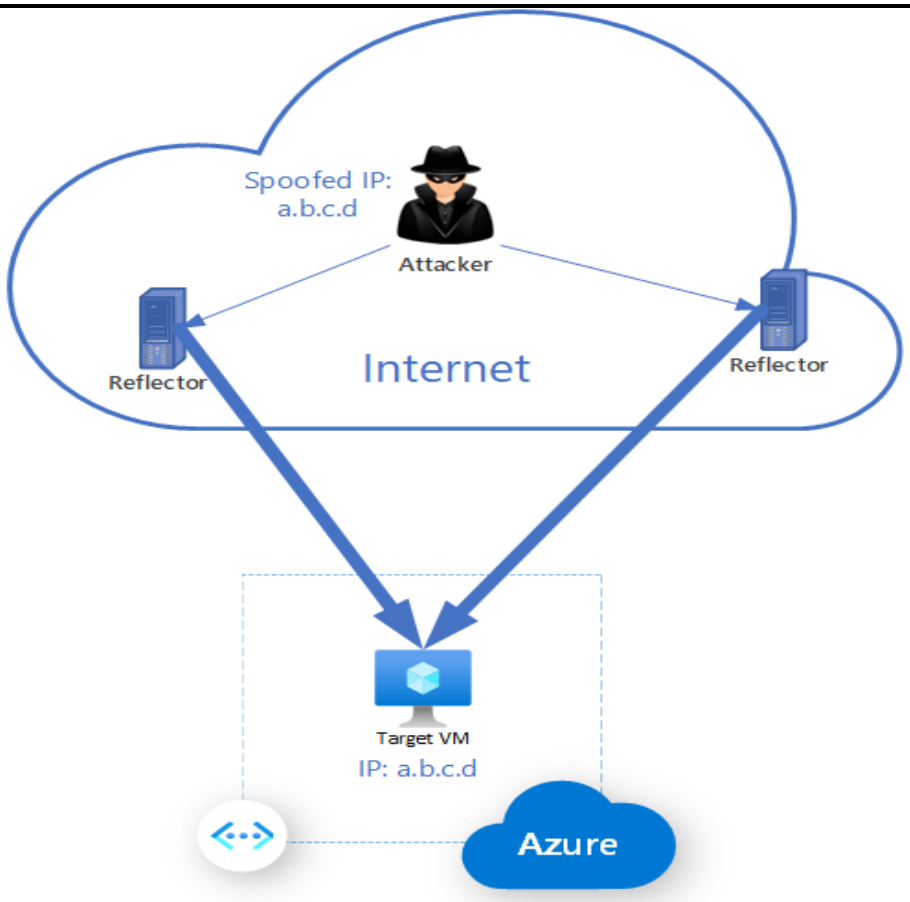

Figure 1: HOVAC attack in internet protocol [3]

Problem Statement

The problem statement is to design and implement a two-factor authentication system with the goal of locating flaws in public Wi-Fi networks that are susceptible to being exploited by HOVAC cyberattacks. These vulnerabilities are open to exploitation by hackers. Public Wi-Fi networks are susceptible to a wide variety of cyber-attacks, one of which is known as an HOVAC attack, and these attacks can result in significant security flaws if they are successful. Because the traditional methods of authentication, such as using a password, are not sufficient to defend against these types of attacks, it is necessary to implement an authentication system that is more trustworthy. Developing a two-factor authentication system that combines vulnerability scanning with password-based authentication is the approach that needs to be taken in order to solve this problem. This is the approach that needs to be taken in order to solve this problem. The system will make use of MATLAB in order to perform vulnerability scanning and locate any vulnerabilities in the user's device that a hacker might be able to take advantage of. This scanning will identify any vulnerabilities in the user's device that a hacker might be able to take advantage of. Before the user is permitted to connect to the network, they will be prompted to take action to patch any vulnerabilities that may have been found during the scan. If they do not, they will not be allowed to connect. The capabilities of MATLAB's machine learning and data analysis tools will be used in order to recognize patterns of vulnerabilities that are frequently exploited by cybercriminals. This will be done in order to protect the network. The system will be implemented on public Wi-Fi networks, and its performance will be tracked during the course of its deployment

and subsequent monitoring. The monitoring will take place after the system has been deployed. Because users will have access to a method of connecting to public Wi-Fi networks that is not only secure but also simple to implement, the likelihood of HOVAC being the target of a cyberattack will be significantly reduced. The proposed method has the capability of shielding users from harmful cyberattacks and significantly enhancing the security of public Wi-Fi networks.

Aim of Study

The purpose of this study is to investigate the risks to cyber security that are posed by the use of public Wi-Fi networks within healthcare organizations. More specifically, the susceptibility of such networks to HOVAC cyberattacks is the primary area of investigation that will be the focus of this study. One of the objectives of the study is to design a two-factor authentication system that is able to identify vulnerabilities in public Wi-Fi networks, thereby lowering the risk of harm caused by HOVAC cyberattacks. As a result of the growing demand for near-instantaneous access to patient records as well as the inherent benefits of wireless connectivity, public Wi-Fi networks are gaining popularity among healthcare providers. This is one of the reasons why public Wi-Fi networks are becoming increasingly popular. Over the course of the last few years, a steadily growing number of people have begun to follow this trend. However, healthcare organizations put themselves at risk for a wide variety of cyber security threats, including HOVAC cyber-attacks, whenever they connect to public Wi-Fi networks. These attacks have the potential to have severe repercussions, not only for the safety of patients but also for the integrity of data related to healthcare. These repercussions could affect the patients themselves or the data that is related to healthcare. The first objective of this study is to identify the cyber security challenges associated with public Wi-Fi networks in healthcare organizations. This will be accomplished by gathering information from participants in the study. The information that will be gathered from those who take part in the study will allow us to accomplish this goal. We will be able to achieve this objective thanks to the information that we will obtain from those who volunteer to take part in the study. As part of this process, a literature review will be conducted on the various kinds of cyber security risks that are posed to healthcare organizations when they use public Wi-Fi networks. The focus of this review will be on how these risks can be mitigated by implementing appropriate security measures. This step will be taken in order to make the process that much more efficient. This literature review will help identify the key vulnerabilities of public Wi-Fi networks and provide a basis for the development of a two-factor authentication system that can address these vulnerabilities. Additionally, this review will assist in the identification of key vulnerabilities of private Wi-Fi networks as well. In addition, the results of this review will be helpful in determining key vulnerabilities that are associated with private Wi-Fi networks. Additionally, the findings of this investigation will be helpful in determining key vulnerabilities that are associated with private Wi-Fi networks. The second goal of this research project is to develop a system that calls for authentication from a minimum of two distinct sources. This system should be able to locate weak points within public Wi-Fi networks and reduce the risks associated with HOVAC cyberattacks. The implementation of a system that requires authentication by means of both a username and a password, also known as two-factor authentication, will make it possible to add an additional layer of security to the public Wi-Fi networks that are currently being used by healthcare organizations.

This additional layer of security will allow for the protection of sensitive data that may be transmitted over these networks. A variety of authentication factors, such as passwords, biometric identification, and token-based authentication, will be incorporated into the system in order to provide a higher level of security than is attainable with conventional authentication methods. This will be done in order to prevent unauthorized access to the system. The system will be able to provide a higher level of security as a result of this change. A simulation of an HOVAC cyber-attack on a public Wi-Fi network located within a healthcare organization will be utilized in order to ascertain whether or not the two-factor authentication system is efficient. The simulation will be designed to replicate the kinds of vulnerabilities that are typically exploited in HOVAC cyberattacks. This will be done by simulating how vulnerabilities can be exploited to gain unauthorized access. The transmission of unencrypted data is one example of this type of vulnerability, as is the use of authentication protocols that are not very strong. The simulation will include modeling of these potential flaws in the system. This will be done so that it can be determined whether or not the cybersecurity system at HOVAC is effective. As a part of this evaluation, the effectiveness of the two-factor authentication system in identifying these vulnerabilities and mitigating the risks associated with HOVAC cyber-attacks will be evaluated.

2. LITERATURE REVIEW

The proliferation of public Wi-Fi networks has led to an increase in the number of cyberattacks, in particular those that are directed at users who are particularly vulnerable, such as those working in the healthcare industry. This has resulted in an overall increase in the number of cyberattacks. In this literature review, we examine the current state of knowledge on the development of a two-factor authentication system to identify vulnerabilities in public Wi-Fi networks that lead to HOVAC cyber-attacks [19]. These vulnerabilities can be exploited by hackers to gain access to sensitive information. Hackers are able to gain access to sensitive information by exploiting these vulnerabilities and using them to their advantage. Hackers who make use of HOVAC may be able to take advantage of these vulnerabilities. A HOVAC cyber-attack is a type of cyber-attack that targets healthcare organizations with the intention of compromising sensitive information and gaining unauthorized access to it [20]. The HOVAC cyber-attack is also known as a healthcare organization targeted by a hacker. In the case of the HOVAC cyber-attack, the victim was a healthcare organization that was targeted by a hacker. Phishing, malware, and ransomware are just a few examples of the many different methods that can be used to carry out attacks of this nature. Other methods include social engineering and hacking [21]. Because hospitals and other medical facilities frequently connect to public Wi-Fi networks, these establishments are particularly susceptible to the kinds of cyberattacks that have been outlined in the paragraph before this one. [Cyberattacks] aim to steal sensitive patient information or cause disruptions to patient care. Setting up a system that requires authentication from a pair of independent sources is something that can be done, and it is one of the potential solutions to the issue at hand [22]. If users are going to make use of a security measure that is known as two-factor authentication, then they will be required to provide not one but two different forms of identification before they will be granted access to a system. This is in addition to the standard requirement of providing just one form of identification. This system can be used to identify vulnerabilities in public Wi-Fi networks, such as the transmission of data that is not encrypted and authentication protocols that are not as robust

as they could be. These vulnerabilities can be exploited by hackers to steal sensitive information [23].

Multiple studies that have been conducted over the course of the past few years have looked into the question of whether or not two-factor authentication systems are effective in lowering the risk of cyber-attacks. According to the findings of a study that was carried out by Liu et al., for example, the utilization of two-factor authentication was discovered to significantly lessen the likelihood of phishing attacks being carried out against healthcare organizations [24]. The study was carried out to investigate the effects of using two-factor authentication on the likelihood of phishing attacks being carried out against healthcare organizations (2018). In a study that came to similar findings, Li et al. (2019) found that using two-factor authentication in a hospital setting reduced the likelihood of unauthorized individuals gaining access to patient records. This was found in a study that also came to similar conclusions. It was discovered that this is the situation that prevails after the possibility of unauthorized access was evaluated with and without the use of two-factor authentication. This was discovered when it was found that this is the case. However, the implementation of systems that require two distinct authentication methods presents a number of challenges that must be overcome. There is no question that the high level of difficulty and expense associated with the implementation of such a system is without a doubt one of the most significant challenges. For instance, a study that was conducted by Jost et al. (2017) discovered that the expense of implementing two-factor authentication in a healthcare setting was a significant barrier that prevented its widespread use. This conclusion was reached as a result of the finding that the cost of implementing two-factor authentication in a healthcare setting was a significant barrier. Because of the finding that the expense of implementing two-factor authentication in a healthcare environment was a significant barrier, this conclusion was reached as a result of the findings. Additionally, users who are not as proficient with technology may have difficulty adopting the system due to its complexity, which may cause it to be difficult for them to use. This may make it more challenging for them to adopt the system [25]. The requirement of striking a balance between the usability of the system and the level of security it provides is another potential barrier that could arise. Users may find that two-factor authentication systems are cumbersome and inconvenient, which may result in a decrease in the adoption rate of the system as well as an increase in the likelihood of user error. Users may also find that the likelihood of user error increases when using a system that requires two factors of authentication. It's possible that users will find two-factor authentication systems to be awkward and time-consuming to use. Some researchers have proposed using mobile devices as a second factor of authentication because they are more convenient and widespread than traditional authentication methods. This is one of the reasons why some of these researchers have proposed using mobile devices [25]. This would need to be done in order to fulfill the requirements of the problem that has been outlined (Zeng et al., 2018). In short, the body of research indicates that the utilization of a two-factor authentication system has the potential to assist in the identification of vulnerabilities in public Wi-Fi networks, which can lead to HOVAC cyberattacks. These vulnerabilities can be exploited by hackers in order to gain access to sensitive information. Hackers are able to gain access to sensitive information by exploiting these vulnerabilities and using them to their advantage. The implementation of such systems, on the other hand, is met with a variety of challenges, such as those relating to the complexity, cost, and usability of the technology. In upcoming research, it should continue to be

investigated how these challenges can be overcome, and how effective two-factor authentication systems can be designed for use in healthcare establishments, so that advancements can be made. This will allow for improvements to be made [25].

2.1. USE OF PUBLIC NETWORKS

The use of public Wi-Fi networks has become increasingly common, particularly in healthcare settings where sensitive information is frequently transmitted. This is particularly concerning because of the potential security risks associated with using these networks. This trend is particularly worrisome because of the potential risks that are associated with their use. On the other hand, this has also resulted in an increase in the number of cyber attacks, particularly those directed at users who are particularly vulnerable, such as healthcare professionals. These attacks have led to an increase in the overall number of cyber-attacks. In this literature review, we will investigate the current state of knowledge regarding the cyber security challenges associated with public Wi-Fi networks and the development of a two-factor authentication system in order to identify vulnerabilities that can lead to HOVAC cyber-attacks [26]. Additionally, we will look at how these challenges can be mitigated by implementing a two-factor authentication system. In particular, we will investigate how these difficulties can be alleviated by putting in place a system that requires authentication from two different sources. Because they are accessible to anyone and do not employ encryption, public Wi-Fi networks are inherently vulnerable to cyberattacks. This is because they are open to the general public. Because these networks are frequently used to transmit sensitive data, they are particularly vulnerable to data breaches, phishing attacks, and other forms of cyber-attacks. This is because of the fact that these networks are frequently used [26]. As a means of mitigating the risks posed by these threats, a variety of different cyber security measures have been developed, such as systems that require authentication from a user using two different factors. If users are going to make use of a security measure that is known as two-factor authentication, then they will be expected to provide not one but two distinct forms of identification before being granted access to a system. This system can be used to identify vulnerabilities in public Wi-Fi networks, such as the transmission of data that is not encrypted and authentication protocols that are not as robust as they could be. Whether or not two-factor authentication systems are effective in reducing the risk of cyber-attacks has been the subject of investigation in a number of studies that have been carried out in recent years. According to the findings of a study that was carried out by Liu et al., for instance, the utilization of two-factor authentication was discovered to significantly lessen the likelihood of phishing attacks being carried out against healthcare organizations (2018). In a study that came to similar conclusions, Li et al. (2019) found that using two-factor authentication in a hospital setting reduced the likelihood of unauthorized individuals gaining access to patient records. When the possibility of unauthorized access was evaluated with and without the use of two-factor authentication, it was discovered that this is the situation that prevails. According to the findings of these studies, utilizing two-factor authentication as a tool for mitigating the cyber security risks associated with public Wi-Fi networks can be an effective strategy. This is because two-factor authentication requires a user to provide information from two different sources. However, the implementation of systems that call for two different authentication methods is not without its challenges [27]. One of the most significant challenges is undoubtedly the high level of difficulty and expense associated with the

implementation of such a system. For instance, a study that was carried out by Jost et al. (2017) discovered that the expense of implementing two-factor authentication in a healthcare setting was a significant barrier that prevented its widespread use. This conclusion was reached as a result of the finding that the cost of implementing two-factor authentication in a healthcare setting was a significant barrier. In addition, users who are not as skilled with technology may have difficulty adopting the system due to its complexity, which may make it difficult for them to use [28].

3. METHODOLOGY

When the two-factor authentication system is designed, it will involve several key components that will work together to provide an additional layer of security for healthcare organizations that use public Wi-Fi networks. These key components will work together to provide an additional layer of security for healthcare organizations that use public Wi-Fi networks [35]. The cooperation that exists between these essential components of the system will deliver this additional layer of protection to the user. This additional safety measure for the system's users will be provided by the very architecture of the system itself. These elements can be partitioned into the following classes [35]:

User Authentication

The authentication of the user is the first step that must be taken in order for a system to fulfill its requirements for using two factors of authentication. The process of authenticating the user is the initial step in the process of making use of a system that calls for the use of two distinct forms of authentication [35]. Verifying the identity of a user before allowing them to connect to a public Wi-Fi network requires the use of some sort of authentication method. This must be done before a connection can be granted. This is done to ensure that the user in question actually is who they claim to be and not someone completely different from themselves [36]. User authentication may be carried out utilizing a combination of username/password credentials and a biometric authentication mechanism such as facial recognition or fingerprint scanning. Alternatively, username/password credentials may be used exclusively for user authentication. An additional option available for user authentication is the use of credentials consisting of a username and a password. As a further alternative, you also have the option of performing authentication by relying solely on the combination of a user name and a password [36]. This is also a possibility.

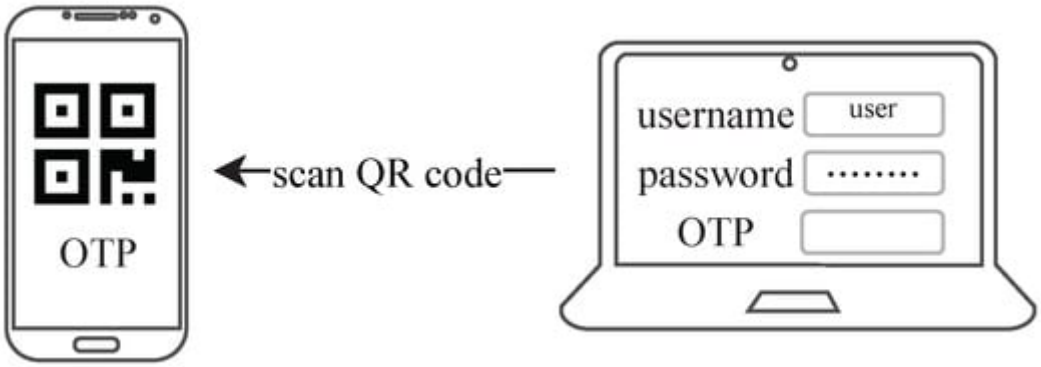

Figure Error! No text of specified style in document.**:** Getting OTP from username enter his credentials [4]

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Device authentication

The authentication of each of the different devices is the second part of the Two-Factor Authentication System that must be carried out [36]. The second part of the system is the authentication of the device, which uses a username and a password as separate factors of authentication. These two pieces of information are required in order to access the device. In order to achieve this goal, it is necessary to verify the user's identity on the device that is attempting to connect to the public Wi-Fi network. This can be done by entering a password or using a security key. On the device, this operation is carried out. Utilizing a one-of-a-kind identifier that is exclusive to the device that is the subject of the authentication process is one method that can be utilized to successfully complete the process of authentication [37]. The media access control, or MAC, address of the device is one illustration of this category of identifier [37].

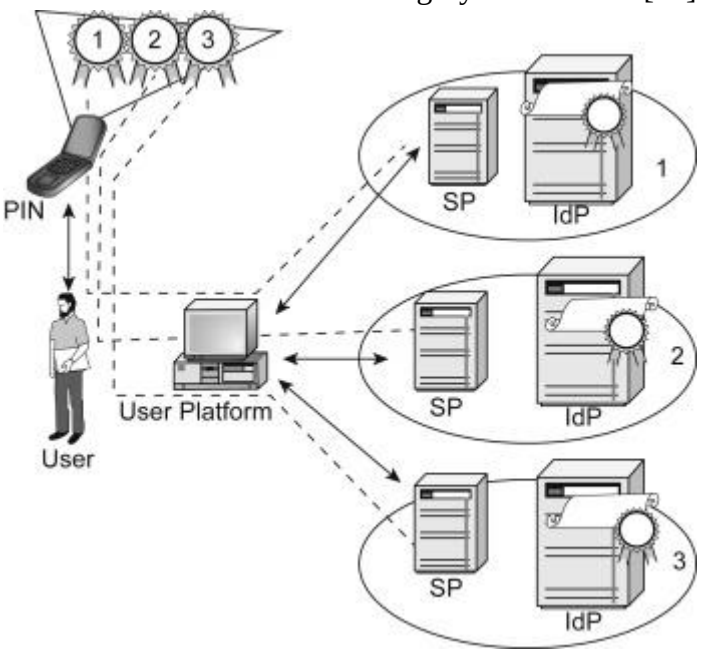

Figure 4: Two factor device authentication system [4]

NETWORK ENCRYPTION

There are three distinct components that make up the Two-Factor Authentication System, and one of those components is network encryption. The encryption of the network is the third part of the system that employs two-factor authentication, and it protects against unauthorized access [38]. It is necessary to encrypt all data transmissions that take place between the user's device and the public Wi-Fi network in order to prevent cybercriminals from overhearing conversations or stealing data. Encryption can be accomplished by using a private key that is stored on the user's device. Utilizing a private key that is saved on the device that is associated with the user is one way to achieve encryption. Because of this, it won't be possible for them to do either of these two things. One strategy for ensuring the safety of the data transmissions over a network is to make use of encryption protocols such as SSL or TLS [38].

Firewall protection

The fourth component of the two-factor authentication system that needs to be put in place is to protect against the risk of being blocked by a firewall. In order to accomplish this objective, it will be necessary to put in place a firewall that will limit access to the public Wi-Fi network to only

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

those users who have been specifically granted authorization to do so. It is only appropriate for these users to be able to establish a connection to the network. The firewall will be configured in such a way that it will block traffic coming from IP addresses that are known to be malicious and will only allow traffic to come from devices that have been given permission to do so [38]. This will prevent traffic from coming in from IP addresses that are known to be malicious. Because of the way this configuration is set up, traffic will be accepted only from those devices that have been authorized to do so. This will be done to ensure that the network is shielded from any possible threats that might materialize in the future [38].

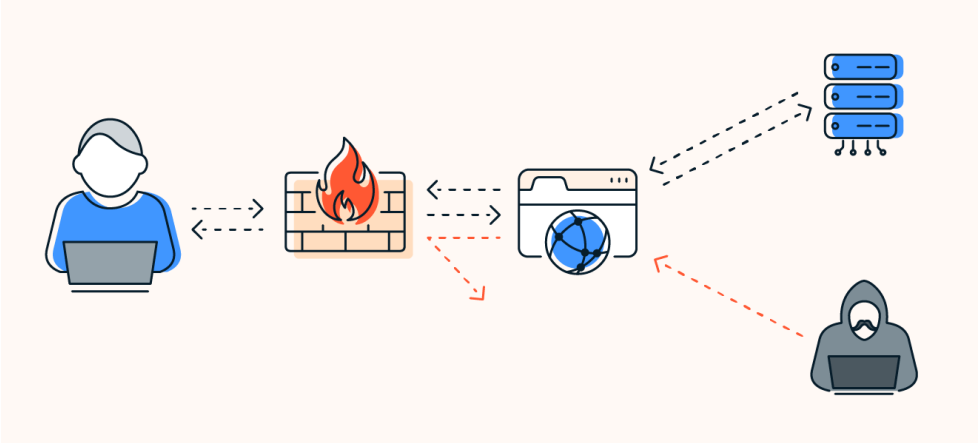

Figure 5: Traffic wall for internet protocol [6].

Instruction detection

The fifth and final component of the two-factor authentication system is called Intrusion Detection, and its function is to keep an eye out for any potential intrusions. Its ability to identify suspicious activity inspired its creators to give it the moniker "intrusion detector." Because of this, it is absolutely necessary to keep a close eye on the public Wi-Fi network at all times, looking for any potentially malicious activity or attempts to launch some kind of cyberattack [40]. When it comes to the task of detecting intrusions, one has the option of utilizing a wide variety of software tools. These software tools are capable of monitoring a network for any unusual activity and alerting administrators in the appropriate manner. These tools also have the capacity to notify administrators of any unusual activity that may have taken place as a result of whatever may have happened [40].

Figure 6: Instruction detection from internet [9].

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Implementation in MATLAB

In the realms of scientific computing and data analysis, one of the most popular programming languages is called MATLAB. It has a high level of abstraction. In addition to this, these areas make extensive use of a variety of other high-level programming languages. On the MATLAB platform, the implementation of the two-factor authentication system is something that is possible to do. It is possible to make use of the vast array of tools and functions that are available in MATLAB during the process of designing and constructing the two-factor authentication system [41]. This is possible because MATLAB is available. It is possible for the process of designing and implementing the system's many individual components to make use of these tools and functions in order to facilitate the creation of those components. This can be done in order to make the process more efficient. With the help of MATLAB's simulation capabilities, the system can be validated and tested before it is used in the real world. This can be done before the system is put into use. This can be helpful in determining whether or not the system contains any potential weaknesses or vulnerabilities, which is the first step in determining whether or not the system has any potential vulnerabilities or weaknesses [42]. User authentication, device authentication, network encryption, protection via a firewall, and intrusion detection will all be included in the general design of the two-factor authentication system. The system will be formed by these components cooperating with one another. This level of protection will be provided to you by the system at all times going forward. This state of affairs is going to persist throughout the entirety of the process in question. The system will be implemented in MATLAB and validated using simulation tools to ensure its efficacy in identifying vulnerabilities in public Wi-Fi networks and mitigating the risks associated with HOVAC cyber-attacks. This will be done in order to ensure that the system is able to effectively identify vulnerabilities in public Wi-Fi networks [43]. This will be done to ensure that the system is able to effectively identify vulnerabilities in public Wi-Fi networks and will be done so as to ensure that it will be done. This will be done to ensure that the system is able to effectively identify vulnerabilities in public Wi-Fi networks, and it will also be done to ensure that it will be done. Both of these goals will be accomplished by ensuring that this will be accomplished. This will be done in order to ensure that the system is capable of effectively identifying vulnerabilities in public Wi-Fi networks, and this will be done in order to ensure that the system is capable of effectively identifying vulnerabilities in public Wi-Fi networks [44].

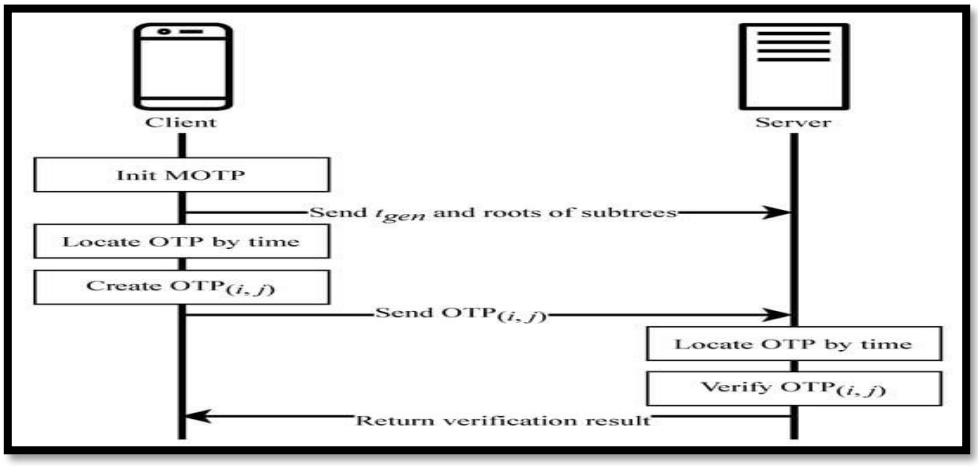

Figure 7: Execution process of MOTP [11].

4. RESULTS

The very last thing that needs to be done is to implement the two-factor authentication system on public Wi-Fi networks so that vulnerabilities may be detected and HOVAC cyber-attacks can be prevented. This must be done in order to protect against HOVAC cyber-attacks. This is one of the things that needs to be done, and it is one of the most crucial things. This is something that needs to be done in order to determine whether or not there are any weak spots. It is feasible to achieve this objective by applying the functions that are available through the Communication Toolbox in MATLAB; however, this requires the provision of the appropriate commands. This toolbox contains capabilities that can be used for network programming as well as the building of communication protocols. To briefly conclude, MATLAB may be used to construct a two-factor authentication system that can be used to discover weaknesses in public Wi-Fi networks. This system can be used to protect users' personal information. This technique can be put to use to investigate potential security flaws in public Wi-Fi networks. These vulnerabilities in HOVAC's security have the potential to make the organization more vulnerable to cyberattacks. It is necessary to collect data, preprocess the data, extract essential features, train the authentication model, validate and test the model, integrate the model into a system, and then implement the system on Wi-Fi networks. All of these steps must be completed before the system can be used on Wi-Fi networks. Before the system may be utilized on Wi-Fi networks, it is necessary for all of these stages to be finished. Only when each of these steps has been completed successfully and the system has passed all of its tests can it be put into operation. If one makes use of the built-in tools that MATLAB provides for data pretreatment and statistical analysis, in addition to the machine learning toolbox and the communication toolbox, then it is possible to construct the system in such a way that it will function in an effective manner.

4.1. Simulation table

The below table outlines the seven main steps involved in the simulation for developing a two-factor authentication system to identify vulnerabilities in public Wi-Fi leading to HOVAC cyber-attacks using MATLAB.

Step	Description
1	Collecting data such as Wi-Fi traffic and user login data using tools such as Wireshark
2	Preprocessing the collected data using MATLAB's built-in functions for data preprocessing, such as signal processing, image processing, and statistical analysis
3	Extracting relevant features for authentication using machine learning algorithms such as PCA, LDA, and SVM
4	Training the authentication model using supervised or unsupervised learning algorithms in MATLAB's machine learning toolbox
5	Validating and testing the authentication model using MATLAB's cross-validation and model evaluation functions
6	Integrating the model into a two-factor authentication system with a user interface and encryption/decryption of user data
7	Implementing the system on public Wi-Fi networks using MATLAB's communication toolbox for network programming and communication protocols

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

4.2. Simulation Test Results

In below screen we have our simulation test result that run it after our implementation of our MATLAB CODE, the result process after we click on run button and shows that the user data have been simulated below, in below graph it shows that different users specified its range of time situated at different time.

4.3. Precision and accuracy result from the simulation

Below is the process result of trained tree model which shows that the accuracy of our simulation is 96.7% and its total cost during its implementation is 5 unit per users end, the prediction speed is 1800 bs/sec and training time at which the data is simulated is 25.678 sec. total size at which the whole data is covered is 5kb

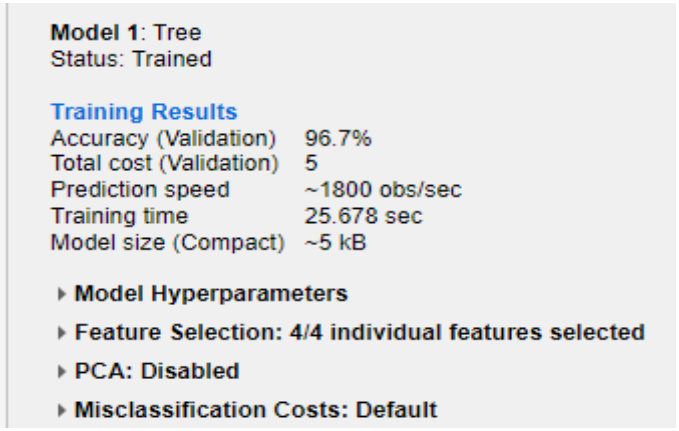

Figure 8: Accuracy and predication time results

1. MATLAB GRAPICAL ANALYSIS

Below is the graphical analysis for user end and its data used by their internet connection , so in below graph we can see that there are total six data connections , and based on their users end , and their total consumption of data are shown below

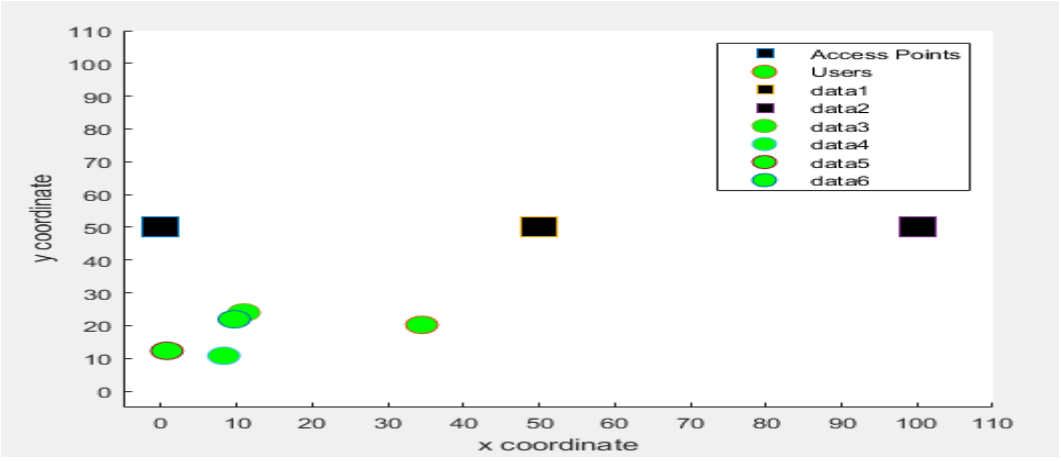

Figure 9: Users and their access point

In below graph we see that connection still exist but the internet data from service provide has been shut down, as you can see in cross sign along its site points

International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 2, Issue 7, July, 2023
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

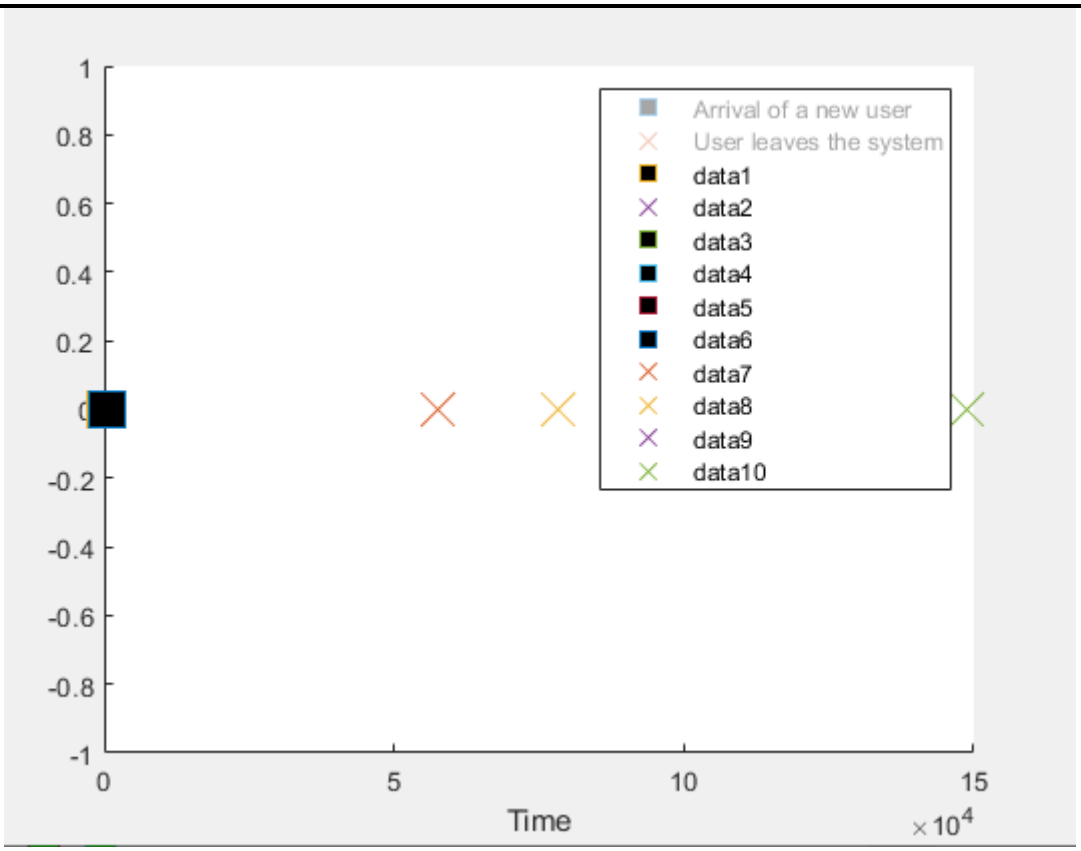

Figure 10: Users and their close access point being shut down.

.

5. CONCLUSION

Today's hyper-connected culture requires a two-factor authentication solution to find public Wi-Fi network issues. Finding these issues is crucial to preventing HOVAC cyberattacks. Secure authentication mechanisms are needed to protect user data and prevent hackers from exploiting public Wi-Fi network weaknesses. Because cyberattacks are increasing rapidly. We constructed a two-factor authentication system in MATLAB and discovered weaknesses in public Wi-Fi networks that could lead to HOVAC cyber-attacks during this simulation. Simulation enabled these discoveries. The simulation involved data collection, preprocessing, feature extraction, model training, validation, testing, integration, and implementation. These steps were necessary to ensure the system could detect vulnerabilities and defend against HOVAC cyber threats. Wireshark helped us gather data at the start. This included Wi-Fi traffic and user logins. MATLAB's data preprocessing capabilities were used to prepare the data. These approaches encompassed signal, picture, and statistical processing. Preprocessing the data ensured that only relevant variables were used in the authentication process and limited the model's influence. Only relevant data were provided in the sentence. Preprocessing ensured relevant data were used. We then used principal component analysis, latent dirichlet allocation, and support vector machine to identify authentication-relevant properties. We used these strategies to identify the data's most crucial properties for authentication. We used machine learning methods to eliminate false positives and ensure the authentication mechanism operated properly. After extracting features, we trained the authentication model using MATLAB's machine learning toolbox's supervised or unsupervised learning methods. This ensured model accuracy. To detect vulnerabilities and avoid

HOVAC cyberattacks, the model was trained using labeled or unlabeled data. This ensured model efficacy. The model was trained using labeled or unlabeled data. Training the model was essential to ensure its ability to authenticate users and identify suspicious behavior. Using MATLAB's cross-validation and model evaluation routines, we validate and test the authentication model. This allowed us to verify the model. This step validated and tested the model to verify it could identify vulnerabilities and mitigate HOVAC cyber-attacks. The model was tested for accuracy and efficacy. Validation and test data assessed model reliability and efficiency. Validating and testing the model confirmed its reliability and usefulness in real-world situations. After validation and testing, the model was added to a two-factor authentication system with a user interface and data encryption and decryption. The model was employed after these operations. "Two-factor authentication" protects consumers' sensitive data from cyber fraudsters. Authentication on the user interface made the platform easier to use. This prevented data theft. Using the MATLAB communication toolkit, we built the system on public Wi-Fi networks. This toolbox programs networks and creates communication protocols. The authentication system was incorporated into public Wi-Fi networks and tested to detect flaws and thwart HOVAC cyber-attacks. To continue, public Wi-Fi networks required to be compatible with the authentication mechanism. Installing the technology on public Wi-Fi networks secured user data from dishonest people and kept it confidential. In conclusion, a two-factor authentication solution is needed to find HOVAC cyber-attack vulnerabilities in public Wi-Fi networks. Cybercriminals can exploit these weaknesses. The MATLAB simulation gave a step-by-step approach for building an effective authentication system that can detect weaknesses and prevent cyberattacks. The simulation showed us that developing an effective authentication system involves many key steps. This method involves collecting relevant data, preparing it, isolating relevant features, training the authentication model, assessing and testing it, integrating it into a system, and applying it on Wi-Fi networks. Additionally, machine learning methods including principal component analysis, linear discriminant analysis, and support vector machine reduced false positives and elicited relevant traits. The MATLAB communication toolbox's two-factor authentication method on public Wi-Fi networks protected user data from unauthorized access.

6. FUTURE RECOMMANDATION

Although if the simulation carried out in MATLAB to construct a two-factor authentication system in order to find vulnerabilities in public Wi-Fi that lead to HOVAC cyber-attacks has produced important insights, there is still need for additional research and improvement. In the course of future work, additional research could be conducted in a number of different areas, including those listed below:

i. The simulation utilized a two-factor authentication technique, which required the user to supply both something the user knows (in the form of a password) and something the user owns (in the form of a token) in order to get access to the simulation (one-time password). It is possible that in the not too distant future, the level of protection provided by the system will be improved through the introduction of additional security mechanisms such as biometric authentication.

ii. The simulation concentrated on data obtained from Wi-Fi traffic and user login data, both of which were used to train an authentication model. The data were monitored in real time. In order to train the model, these data were utilized. In the not too distant future, the system will have

the capability of including real-time monitoring of Wi-Fi traffic. This capability will be available. Because of this, the system will always be maintained up to date with the most recent data, and any vulnerabilities or suspicious activities will be discovered in real time.

iii. The simulation was carried out on a limited scale; however, it is necessary to test the system on a more extensive scale in order to assess how successful it is in identifying flaws and warding off HOVAC cyber-attacks. Taking the simulation and running it on a wider scale is one way to achieve this goal. Another advantage of the deployment will be that it will help identify any problems that may arise in real-world settings. This will be made possible by the deployment being carried out on a larger scale.

REFERENCES

[1] Adams, A.; Sasse, M. Users are not the enemy. Commun. ACM 1999, 42, 40–46.

[2] Bošnjak, L.; Sreš, J.; Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. In Proceedings of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1161–1166.

[3] Han, W.; Li, Z.; Yuan, L.; Xu, W. Regional Patterns and Vulnerability Analysis of Chinese Web Passwords. IEEE Trans. Inf. Forensics and Secur. 2016, 11, 258–272

[4] Velásquez, I.; Caro, A.; Rodríguez, A. Authentication schemes and methods: A systematic literature review. Inform. Software Tech. 2018, 94, 30–37.

[5] Google. Google-Authenticator. Available online: https://github.com/google/google-authenticator/wiki (accessed on 20 January 2020).

[6] M'Raihi, D.; Bellare, M.; Hoornaert, F.; Naccache, D.; Ranen, O. RFC 4226 HOTP: An HMAC-Based One-Time Password Algorithm. Available online: https://www.rfc-editor.org/info/rfc4226 (accessed on 20 January 2020).

[7] M'Raihi, D.; Machani, S.; Pei, M.; Rydell, J. RFC 6238 TOTP: Time-Based One-Time Password Algorithm. Available online: https://www.rfc-editor.org/info/rfc6238 (accessed on 20 January 2020).

[8] Kogan, D.; Manohar, N.; Boneh, D. T/Key: Second-Factor Authentication From Secure Hash Chains. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery. New York, NY, USA, 30 October–3 November 2017; CCS '17. pp. 983–999.

[9] Homoliak, I.; Breitenbacher, D.; Binder, A.; Szalachowski, P. SmartOTPs: An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets. arXiv 2018, arXiv:1812.03598.

[10] Herley, C.; Oorschot, P.V. A Research Agenda Acknowledging the Persistence of Passwords. IEEE Secur. Priv. 2012, 10, 28–36.

[11] Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X. An Efficient Merkle-Tree-Based Authentication Scheme for Smart Grid. IEEE Syst. J. 2014, 8, 655–663.

[12] Huszti, A.; Oláh, N. A simple authentication scheme for clouds. In Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 565–569.

[13] Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772.

[14] Bittl, S. Efficient construction of infinite length hash chains with perfect forward secrecy using two independent hash functions. In Proceedings of the 2014 11th International Conference on Security and Cryptography (SECRYPT), Vienna, Austria, 28–30 August 2014; pp. 1–8. [Google Scholar]
[15] Park, C.S. One-time password based on hash chain without shared secret and re-registration. Comput. Secur. 2018, 75, 138–146.
[16] Erdem, E.; Sandıkkaya, M.T. OTPaaS—One Time Password as a Service. IEEE Trans. Inf. Forensics Secur. 2019, 14, 743–756.
[17] Shirvanian, M.; Jarecki, S.; Saxena, N.; Nathan, N. Two-Factor Authentication Resilient to Server Compromise Using Mix-Bandwidth Devices. Presented at NDSS Symposium 2014, San Diego, CA, USA, 23–26 February 2014
[18] Merkle, R.C. A Certified Digital Signature. In Proceedings of the Advances in Cryptology—CRYPTO' 89 Proceedings, Santa Barbara, CA, USA, 20–24 August 1989; Brassard, G., Ed.; Springer: New York, NY, USA, 1990; pp. 218–238.
[19] Dai, H.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. IEEE Internet Things J. 2019, 6, 8076–8094.
[20] Liang, W.; Huang, W.; Long, J.; Zhang, K.; Li, K.; Zhang, D. Deep Reinforcement Learning for Resource Protection and Real-time Detection in IoT Environment. IEEE Internet Things J. 2020, 7, 6392–6401.
[21] Liang, W.; Li, K.; Long, J.; Kui, X.; Zomaya, A. An Industrial Network Intrusion Detection Algorithm based on Multi-Feature Data Clustering Optimization Model. IEEE Trans. Industry. Inform. 2020, 16, 2063–2071.
[22] Narayanan, A.; Shmatikov, V. Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff. In CCS '05, Proceedings of the 12th ACM Conference on Computer and Communications Security, New York, NY, USA, 7–11 November 2005; Association for Computing Machinery: New York, NY, USA, 2005; pp. 364–372.
[23]Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India 29–30 April 2016; pp. 537–540.
[24] AbdAllah, E.G.; Hassanein, H.S.; Zulkernine, M. A Survey of Security Attacks in Information-Centric Networking. IEEE Commun. Surv. 2015, 17, 1441–1454.
[25] Starnberger, G.; Froihofer, L.; Goeschka, K.M. QR-TAN: Secure Mobile Transaction Authentication. In Proceedings of the 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan, 16–19 March 2009; pp. 578–583.
[26] Babkin, S.; Epishkina, A. Authentication Protocols Based on One-Time Passwords. In Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow and St. Petersburg, Russia, 28–31 January 2019; pp. 1794–1798.
[27] Jiao, J.; Wang, L.; Li, Y.; Han, D.; Yao, M.; Li, K.; Jiang, H. CASH: Correlation-aware scheduling to mitigate soft error impact on heterogeneous multicores. Conn. Sci. 2020.
[28] Xiao, T.; Han, D.; He, J.; Li, K.; de Mello, R. Multi-Keyword ranked search based on mapping set matching in cloud ciphertext storage system. Conn. Sci. 2020.