As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(01): 240-245, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0801042
Available online at: http://www.ijmtst.com/vol8issue01.html

Vulnerabilities and Threats to the Network Security in Wireless Cloud

Ajay Nanwatkar | Dr. Liladhar Rewatkar

Assistant Professor, Department of Commerce, Prerna College of Commerce, Nagpur, MS, India.

To Cite this Article

Ajay Nanwatkar and Dr. Liladhar Rewatkar. Vulnerabilities and Threats to the Network Security in Wireless Cloud. *International Journal for Modern Trends in Science and Technology* 2022, *8* pp. 240-245. https://doi.org/10.46501/IJMTST0801042

Article Info

Received: 09 December 2021; Accepted: 06 January 2022; Published: 12 January 2022.

ABSTRACT

Wireless security is about preventing unauthorized access or interference with computers that use wireless networks. Wireless network security has been the subject of research for the past two decades without any previous solution to the security methodology used to prevent unauthorized access to data. The aim of this study was to review some of the wireless security literature on attacks, threats, vulnerabilities, and solutions to these problems. Cloud Computing (CC) is a promising technology due to its common characteristics such as online storage, high scalability, and seamless access, as it plays a key role in lowering capital and labour costs and enables companies to conduct their business and finances in the cloud. While CC is a great innovation in terms of easy-access computers, it has some limitations. As the use of the cloud increases, security concerns are proportional to the increase.

KEYWORDS:Wireless Network, Network Security, WAP2, WEP, Security; Privacy; Integrity; Non-Repudiation; Threats; Green Consequences.

1.INTRODUCTION

Wireless network is a configured network that uses the frequency of the radio signal to communicate between computers and other network devices, it is sometimes called a Wi-Fi or WLAN network, and it is becoming more and more popular nowadays because of the simple configuration function and the lack of wiring. Wireless Internet access technology is gradually being implemented in offices and public facilities, as well as by Internet users in the home.

Due to continuous technological progress paired with increasing price / performance advantages, wireless accessibility is increasingly being implemented in offices and public environments. This new era of technological flexibility can also be an open invitation to threats to network security not only in the corporate world but also to the privacy of the users at home.

When deciding to move from a physically connected architecture to wireless LAN technology, component accessibility and signal propagation provided unauthorized users with practical opportunities to introduce malicious activity, intercept data transmissions, or passively intercept a system's infrastructure. Security is about preventing unauthorized access or damage to computers that use wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA). It requires a different way of thinking about the security of wired networks, as it allows hackers or attackers easy access to means of

transport and this access increases the threat to any security architecture. Wireless security over the IEEE 802.11 standard has received a lot of criticism because it has different designs has flaws and security issues.

Edge computing is an emerging technology to bring compute and storage resources closer to the data source, increase response times, and conserve limited bandwidth in response to the rapid growth of the IoT and increasing demand for advanced applications and services. However, security, privacy and data protection at edge nodes in the computing world are significant challenges due to the limited resources available and the large amount of sensitive user data at the edge nodes. Conventional CC used to support general IT systems cannot meet the needs of IoT and mobile services due to problems such as lack of location, bandwidth limitations, high operating costs, lack of services and data protection issues. These DC constraints open up opportunities for advanced computing where this technology is engineered globally to meet the runtime and growing real-time demands of IoT and mobile devices or nodes.

Figure 1- Cloud Computing Model

2. RELATED WORK

In recent years, advances in network-based computing and mobile cloud computing (MCC) applications have emerged as potential technology for mobile services. It is the combination of mobile computing, cloud computing, and wireless networks to deliver high quality. Computing resources for network operators, cell phone users and cloud computing providers [1, 2]. MCC is a new platform to combine mobile devices and cloud computing to create a new infrastructure. It refers to an infrastructure in which both data storage and data processing takes place outside the mobile device [3]. In this architecture, the cloud takes over the heavy computing tasks and stores large amounts of data. The rapid emergence of mobile computing (CM) [4] is becoming a strong trend in the development of information technology. However, in mobile computing, mobile devices face many problems with regard to their resources (e.g., battery life, storage and bandwidth) and communication (e.g., mobility and security) [5].

Due to the important application model in the Internet age, mobile cloud computing has become an important research topic of scientific and industrial communities, its application is becoming more popular day by day, so that they have developed and operated various applications based on mobile cloud computing for users such as Google Maps , Gmail and navigation systems for mobile devices, voice search and various applications on an Android platform, Apple's MobileMe and Motorola's Moto Blur. The growing application of mobile computing emerges from a study by Juniper Research which finds that the consumer and business market for various cloud-based mobile applications is $ 9.5 billion [6]. The main goal of cloud computing is to provide various services, software and processing capacities over the Internet, increasing storage space, reducing costs, automating systems and decoupling the provision of services from the underlying technology, as well as providing flexibility and Mobility of information for various purposes. Fig. 1: Mobile cloud computing Mobile cloud applications shift computing power and data storage from cell phones to the cloud. Powerful and centralized computer platforms in clouds over the Internet. All of these centralized applications are then accessed via the wireless connection based on a thin native client or web browser on mobile devices. Alternatively, mobile cloud computing can be defined as a combination of web mobile devices and cloud computing [8, 9], the most popular tool for mobile users to access applications and services on the Internet.

3. PRIVACY AND SECURITY MODELS OF CC AND RELATED CONCEPTS

A.Security and Privacy Issues in CC

Researchers recently suggested that when the cloud is used for a variety of purposes, such as storing data, it would put your sensitive data there and allow users to

access tools on the network. Communication, such as email and calendar, with different tools., Microsoft Office and Google Docs, via the Internet, for application development and also for testing the application and its use by companies, as well as for data backup and recovery. Therefore, privacy and security are very important. Users use the cloud for different purposes. The data is infinite beyond the control of the data server. Their ignorance of the data owner is how the information is used and where it is stored. In this way, data owners need more rights about their data, such as:

B. Issues in Cloud Services

The data is stored in a cloud. The CSP takes care of the integrity and confidentiality of the data. The CSP carries out an audit of the data and an audit by external auditors (TPA) at a certain interval. TPAs have verified cloud data; check the accuracy of the data; as a check they do not see all user data, but there is a possibility that data protection will be lost.

C. Data Verification in the Cloud

Cryptographic algorithms for verification of data in the cloud are used to guarantee the integrity and confidentiality of the data. Cell phones have limited resources; H. Limited battery, low computing power, low storage capacity, etc. At that time, mobile devices have become a personal necessity. Cell phone performance can be increased by integrating the cloud with a cell phone called CC Mobile. All functions are performed in the cloud and with few resources on mobile devices, users can get great functionality. But the wireless network manages the communication between the cloud and the mobile device. Therefore, there is a great challenge of data protection and the security of user data. For data security, "Distributed Multi-cloud Storage", "Data Encryption" and "Data Compression" can be used in Mobile CC. The data is divided into different parts, which encrypt this data and send it to distributed clouds to store the large amounts of data.

D. Health Data Confidentiality Issue

In medical records, maintaining confidentiality of personal attributes has become a difficult task. Various techniques have been proposed to overcome this problem, such as verbose exchanges and attribute-based encryption (ABE). An encryption scheme is offered that supports online / offline validity and also reduces the computational effort. In the ad hoc customer centre, the distribution of tasks is a challenge. Server location and quality of service (QoS) are challenges. In order to achieve differential data protection (DP), the RPSD scheme was introduced, which ensures efficient site data protection and QoS. Using a geocaching mechanism goes beyond the search strategy.

E. IoT and Cloud Integration

However, some common points of interest have been recognized in writing for their combination. From one perspective, the IoT can use essentially unlimited capabilities and cloud-based resources to meet its mechanical requirements (e.g., capacity, availability, and dynamics). In particular, the cloud offers a successful offer for IoT-based management, administration and creation, such as B. Components and applications that promote things or information they create. In addition, the cloud benefits from the IoT by expanding its ability to handle authentic things in a more distributed and dynamic way, and by leveraging new authorities and directions in immeasurable living conditions.

F. Cellular Devices in CC

Mobile devices such as cell phones are gradually becoming an indispensable part of individuals' daily lives, encouraging them to perform a wide variety of useful tasks. Mobile distributed computing environments coordinate flexible recordings and the cloud to expand their capabilities and help utilize and overcome their limitations such as limited storage, storage capacity and more. Handling and battery life. Network health analytics and the role of Mobile CC along with data analytics in the activation process.

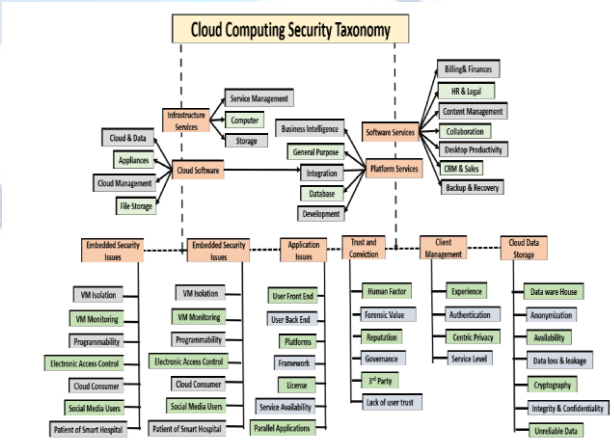

Figure 2- Classification of Cloud Computing and cloud security

4. DÉFENSE MEASURES AGAINST SECURITY THREATS AND ATTACKS

End-to-end security solutions between CSP and CSC include Internet-specific security solutions such as SSL / TLS (e.g., HTTPS) or VPN access to the cloud (with IPsec). Another possibility for the application layer security mechanism is the use of PKI (Public Key Infrastructure) for the cloud. Consumer managed access control requires less trust in the CSP. In this case, the Policy Decision Point (PDP) is in the CSC domain and the Policy Enforcement Point (PEP) is in the CSP domain. In theory, the steps should be to minimize the lack of security, privacy and trust policies, the loss of surveillance control, the certification of lack of trust, the loss of control when using different clouds, multi-user use in the cloud, etc.

The minimization of the lack of security, data protection and trust policies are emphasized by consumers, who make clear demands for protection and security, so that they do not have a say in how to react; This is where the location of the provider or the provided cloud service comes into play. Currently, consumers cannot tell the service provider what they want (SLAs are one-sided). A standard policy statement is required to communicate your policies and goals. All parties agreed and it was confirmed. SLAs are presented using standard vocabulary. to achieve a general security situation in an environment within the cloud by creating policy instructions that contain basic functions, such as an understandable (or at least controllable) machine. [10]

It's easy to combine, integrate, and compare; However, there is a need to develop separation between virtual machines, require geographic isolation between virtual machines, and so on. These are the different examples of different policy statements. A validation tool is also needed to verify that the policy created in the default language correctly reflects the intentions of the policy maker (i.e., the policy language is semantically equivalent to the intentions of the users). To reduce the lack of trustworthy certifications, certification or some form of trustworthy and independent benchmarking and a detailed description of the security is required. and warranty functions, Sarbanes Oxley, DIAC App, DISTCAP, etc. (Is that enough for a cloud environment?) And a third-party certified risk assessment provides additional security for the consumer cloud.

5. AGGREGATE / COMPREHENSIVE CC CHALLENGES

Various challenges can be summarized in three categories.

i. Cloud service customers- These are ambiguities in responsibilities, loss and mistrust, security and data protection, unavailability of the service, blocking of the cloud service provider, misappropriation of data and intellectual and sensitive property, loss of governance, control and software. Integrity.
ii. Cloud service provider- Uncertainty in management, responsibility and administration in shared cloud environments, inconsistency and conflict in data protection and security measures, conflicts of responsibility, evolutionary risks, bad and bad migration process, integration, business interruption, cloud blocking of service partners, weak points in the supply chain, software dependencies.
iii. Cloud Service Partner- These are ambiguities related to the responsibility, control, regulation and misappropriation and counterfeiting of intellectual property.

6. VULNERABILITIES AND THREATS IN NETWORK SECURITY

To properly ensure the integrity of a network, administrators need framework standards to implement various protocols. To replace TCP / IP and to meet this requirement, the Open Systems Interconnection (OSI) model was introduced as a network reference model for analysing data communication between hardware and software in a seven-level system. When performing truly unique tasks, each tier is also assigned to support the upper tier and provide services to the lower tier.

	OSI Model : 7 Layers & Architecture			
	Assigned Layer Number	*Data units type*	*OSI model layer*	*Layer function*
Host Layers	7	Data	Application	• Applications interface • Interpreting program requests & info requirements.
	6	Data	Presentation	• Data compression • Data representation • Encryption.
	5	Data	Session	• Communications of interhost
Media Layers	4	Segments	Transport	• End-to-end connections • Properly sequence of packets
	3	Packets / datagram	Network	• Establish network connection • Translate network addresses • Transmitting individual packets across a network • Logical addressing: IP.
	2	Bit / frames	Data link	• Physical addressing
	1	Bits	Physical	• Physical network connection signal management • Binary bit transmission • Media

A. *Physical Layer Vulnerabilities includes-* Power failure, loss of control of the environment, physical theft of data and hardware, physical damage or destruction of data and hardware, unauthorized changes in the functional environment (data connection, removable media, add / remove resources), disconnect connections from physical data, data interception and not detectable keystrokes and other input records.

B. *Link Layer Vulnerability includes-* MAC address spoofing (station confirms the identity of another), VLAN bypass (station can force direct communication with other stations, bypass logical controls such as subnetworks and gateways), spanning tree errors can be introduced accidentally or on purpose Layer 2 creates environments that cause packets to loop endlessly, in wireless media situations, Layer 2 protocols can allow unauthorized entities to freely connect to the network, or authentication and weak encryption can create a false sense of security. Ports that allow data to be intercepted by any device connected to a VLAN.

C. Network Layer Vulnerabilities includes- Phishing routing, malicious distribution of network topologies, IP address spoofing, incorrect source routing in malicious packets, identity and resource ID vulnerabilities.

D. Transport Layer Vulnerabilities includes- Incorrect handling of unknown, unknown or "illegal" conditions, differences in transport protocol implementations that allow “fingerprints" and other host information enumerations, overloading of transport layer mechanisms such as transmission mechanisms can be based on specially designed packets and estimated illuminated traffic and transmission values falsified and attacked, which enables the interruption or control of communication.

E. *Session Layer Vulnerabilities includes-* Weak or nonexistent authentication mechanisms Transmission of session data such as user ID and password in clear text that enables interception and unauthorized use, session identification can be prone to spoofing and hijacking, Loss of information due to failed authentication attempts, failed sessions Allow unlimited brute force attacks on credentials.

F. *Presentation Layer Vulnerabilities includes-* Poor handling of unexpected input can lead to us crash or give up control over the execution of arbitration proceedings and instructions. The unintentional or reckless use of externally provided inputs in control contexts can enable remote manipulation or the loss of information; cryptographic errors can be exploited to circumvent data protection.

G. *Application Layer Vulnerabilities includes-* Open design issues allow unintended parties to use application resources for free, backdoors and application design flaws circumvent standard security controls, inadequate security controls enforce "all or nothing" leading to excessive or inadequate access, overly complex application security controls tend to be bypassed or misunderstood and implemented Gaps in program logic are accidentally or intentionally used to lock programs or to cause inappropriate behaviour.

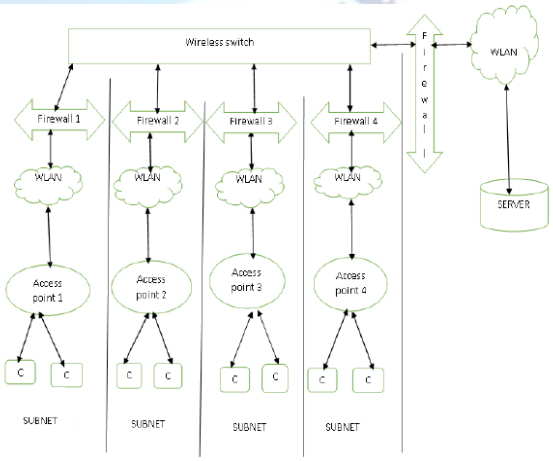

Figure No 3: Suggested solution for small organization wireless network

Firewall 1 is responsible for protecting the computers in Access Point 1 from attacks by computers from other Access Points, the same applies to Firewalls 2, 3 and 4. [11]

7. FUTURE SCOPE AND CONCLUSION

There always seem to be difficulties with the wireless one Completely secure the network against attacks, threats and vulnerabilities. The purpose of this study was to visit various wireless network security publications and to suggest network security solutions that can protect the wireless network better than existing solutions. Most publications have indicated that securing a completely wireless network is not an easy task, but parts of that network can be secure, but not the entire network. Therefore, this study suggests Figure 3, although it is expensive, but it can protect part of the network as it poses a challenge to the attacker visiting each node to access the entire network, which could lead to the detection of an attacker. In addition, it is recommended that future research on security and privacy in CC-based smart cities focus on solving the challenges identified and discussed in this review, which will be beneficial for reaching and establishing other smart initiatives without exception city in different CC environments.

REFERENCES

[1] S. Abolfazli, Z.Sanaei, E. Ahmed, A.Gani and R, Buyya, R. In: Cloud-based augmentation for mobile devices: motivation, taxonomies, and open challenges. Communications Surveys & Tutorials, IEEE, 16(1), 2014, pp. 337-368.

[2] F, Liu, P. Shu, H. Jin, L. Ding, J. Yu, D.Niu and B. Li. Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. Wireless Communications, IEEE, 20(3), 2013, pp. 14-22.

[3] S. Perez, why cloud computing is the future of mobile,http://www.readwriteweb.com/archives/why cloud com putting is the future of mobile php, Retrieved on February 2015.

[4] M. Satyanarayanan. Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond (MCS), 2010.

[5] P.Tavel. Modeling and Simulation Design. AK Peters Ltd 2007.

[6] S. Perez, Mobile cloud computing: $9.5 billion by 2014, http://exoplanet.eu/ catalog.php, 2010.

[7] White Paper. Mobile Cloud Computing Solution Brief. AEPONA, 2010.

[8] J. H. Christensen."Using RESTful web-services and cloud computing to create next generation mobile applications," Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, ACM, 2009, pp. 627-634.

[9] L. Liu, R.Moulic and D. Shea. "Cloud service portal for mobile device management",E-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on IEEE, 2010, pp. 474-478.

[10] Z. Tari. "Security and Privacy in Cloud Computing", IEEE Cloud Computing, 1(1), pp.54-57. [11] Branstad, D., 1987. Considerations for security in the OSI architecture. IEEE Network, 1(2), 2014, pp.34-39.

[11] D. Branstad. Considerations for security in the OSI architecture. IEEE Network, 1(2), 1987, pp.34-39.