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): 97-103, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0801018
Available online at: http://www.ijmtst.com/vol8issue01.html

Check for updates

Security and Authorization Issues in Wireless Network Cloud

Chandrashekhar Tople | Dr.Liladhar Rewatkar

Assistant Professor, Prerna College of Commerce, Nagpur, Maharashtra, India

To Cite this Article
Chandrashekhar Tople and Dr.Liladhar Rewatkar. Security and Authorization Issues in Wireless Network Cloud. *International Journal for Modern Trends in Science and Technology* 2022, *8* pp. 97-103. https://doi.org/10.46501/IJMTST0801018

Article Info
Received: 24 November 2021; Accepted: 31 December 2021; Published: 05 January 2022

ABSTRACT

The wireless cloud is in high demand and used by almost every business. The interest of organizations in cloud computing has sparked a primary desire to become more efficient and effective with information technology (IT). Mobile Cloud Computing (MCC) is a Combination of Mobile Computing, Cloud Computing, and Wireless Networking Mobile cloud computing is gaining increasing interest due to its wide applicability in a variety of social, industrial and commercial mobile applications. Mobile and smart devices can share complex compute operations with cloud service providers (CSPs). It also ensures archiving, the application of access policies and security operations. In many cases, CSP requires the services of contributors' CCs for data collection, sharing, and mobile application support. This requires trust management for CCs to protect themselves from malicious CCs and ensure data security and privacy. However, end users or data requesters also need reliable security solutions to share their data or access to unknown DC data. In recent years, information communication and computer technologies are deeply converging, and various wireless access technologies have been successfully implemented. Mobile cloud computing embodies the paradigm of cloud computing in the mobile environment, the set of technologies that allow you to access network services anywhere, anytime, anywhere. This addresses many technical challenges, such as low bandwidth, availability, heterogeneity, e-downloads, data access, security, privacy, and trust. We also identify the beginnings of a promising wireless network security architecture, which focuses on a process of authentication, authorization and access control in the wireless cloud. This article presents the study of security and authorization issues in the wireless cloud.

KEYWORDS: Wireless Network Cloud, Cloud Computing, Computing Security, Authorization.

1.INTRODUCTION

This system uses emerging cloud computing technology and various technologies involved in wireless infrastructure. Wireless communications have developed rapidly in recent years. They have had a huge impact on all aspects of the work of people, society and the economy. This easily leads to the Informatica cloud which allows consumers, small and large businesses, enterprises and governments to easily access IT resources with little or no effort, investment or upfront commitment [1]. mobile environment, the set of technologies that allow people to access network services anywhere, anytime, and anywhere. smartphone users. Integration of cloud computing and mobile devices, networks face many technical challenges, such as low bandwidth, availability, heterogeneity, processing offload, data access, security, privacy and trust, all dictated by the dramatic increase in the use of smartphones in recent years. [2].

To be confident in a wireless cloud deployment, having sufficient visibility to see who is doing what and how in the infrastructure is essential. This means the use of governance or the ability to monitor, manage, and control all aspects of the architecture, including the ability to trace security issues to the source of the issues. In this article, we have highlighted some issues related to security as well as privacy in cloud applications [3].

2.CLOUD COMPUTING

Cloud computing is a style of computing in which dynamically scalable resources are virtually delivered to customers as a service over the Internet.

The definition and practical implementation of Cloud require it to have the following key characteristics:

- Virtualization
- Scalability
- Usability
- Reliability
- Security
- Cost

Cloud Computing being mainly driven by professional use, it must have an economic model based on the pricing of customers for use services. As a result, cloud service providers typically adopt some form of the pay-as-you-go model. Cloud Computing services are broadly divided into the following three main categories, and a stack of these services is shown in Figure 1.

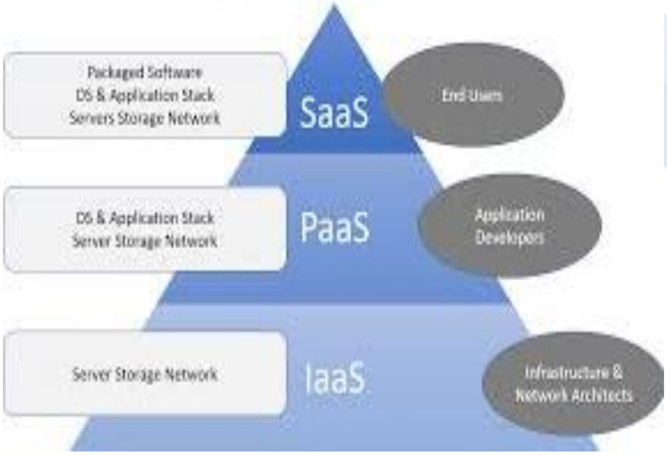

Figure 1- Cloud Service Model [4]

3.THE WIRELESS NETWORK CLOUD

The Wireless Network Cloud (WNC) is a disruptive technology and system architecture for the next generation wireless access network. This system uses emerging cloud computing technology and various technologies involved in wireless infrastructure, such as Software Defined Radio (SDR) technology and Remote Radio Head (RRH) technology [5].

Therefore, in a wireless cloud environment, organizations will move from perimeter security models to a service level view of security. The focus should be on network identities, trust and authorization of users and applications rather than ownership and control. The architectural model of a wireless cloud computing environment is identified in Figure 2, [6] identified the wireless cloud as a natural extension of the wireless network. It provides uninterrupted access to the Internet, network devices and computing capabilities. The wireless cloud is a kind of next-generation wireless network, and as an emerging technology there is very little literature on it [7].

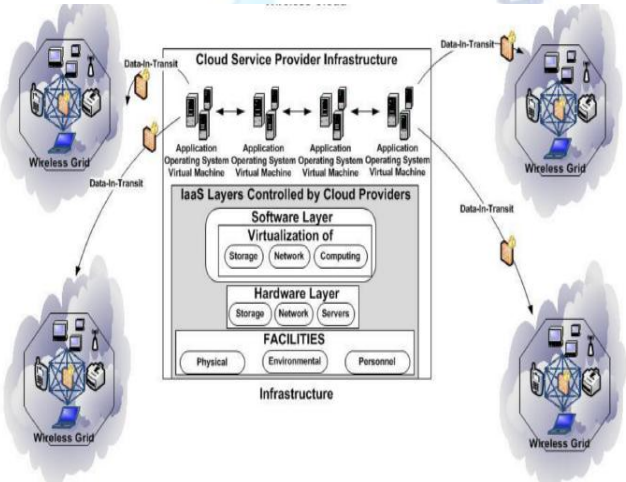

Figure 2- Wireless Network Cloud

With the advancement of cloud and wireless technology, the architecture wireless cloud can evolve from a distributed and decentralized architecture with lots of data in "thin" access points (AP) to a centralized architecture using "thick" access points with data located in wireless switches. When considering the risks associated with a wireless cloud architecture, the most fundamental thing to consider is how the wireless cloud environment affects the trust model. What happens when applications move to a wireless cloud where the business model is typically based on providing common services to a wide variety of customers. At this point, the security of these applications and their data is largely dependent on the skill, willingness, diligence and ability of the wireless service provider to protect the data and provide reliable service. poses a significant challenge from an information security perspective.

4.VULNERABILITIES AND THREATS TO THE WIRELESS NETWORK CLOUD

As data moves through the wireless cloud, privacy and data integrity controls should be applied to limit exposure to unauthorized users. Knowledge of information security threats is very useful for system administrators, testers, and information security professionals, who need to understand how information systems can be attacked. The intention of a threat is to exploit a vulnerability of a weak point in an information system. In any risk assessment, threats must first be identified. CNSS instruction 4009 [9] defines a threat as any circumstance or event having a potential negative impact on the operations of the organization (including the mission, function, image or reputation), the resources of the organization. organization, individuals, other organizations or the Nation via an information system via unauthorized access, destruction, disclosure, modification of information and / or denial of service (DoS) attack. Unlike a wired network, the wireless cloud is not limited by physical space. This potentially opens the network to attacks from unauthorized users who spy on wireless broadcasts or gain unauthorized network access from inside or outside [10]. Traditional thieves, hackers, high tech criminals, government sponsored organizations, viruses and other types of malicious code are typical causes of security problems in wireless networks [11].

The targets of the attacks are files stored on hard drives and other media, data and voice communications transferred between remote clients and internal networks, or the remote system, as used to access the main network. There are vulnerabilities in wireless networks that are interconnected with any other system. The entire network becomes more vulnerable because when one part of the system is compromised, the rest of the network can also be affected. Even unsecured wireless communications equipment is vulnerable to vandalism and terrorism which can cause large-scale communications disruption. The extent of any attack on a wireless network depends on the type of network, network security precautions, the location of the network, and the skills of the adversary who wants this information. Any vulnerabilities that exist in a conventional wired network will apply to the wireless cloud. Malicious entities can gain unauthorized access to a given computer network over wireless connections, bypassing any firewall protection, and can steal the identity of legitimate users and hide them on internal networks [12]. These entities may be able to invade the privacy of legitimate users by tracking their movements or using untrusted third-party wireless network services to access network resources. Malicious code or viruses can corrupt data on a wireless device and then be introduced into a wired network connection. While it is more difficult and potentially more important to secure wireless communications, the respective issues, threats, and services required to adequately respond to these threats are mostly the same for both wired and wireless technologies. Managing security threats and vulnerabilities in information system assets are two key challenges for organizations [13].

Security engineers can reduce the risks associated with systems by identifying threats and making design or procedural changes to a system to reduce its vulnerability to those threats. This article identifies potential threats to a wireless cloud environment that can be used as a starting point to secure a wireless cloud architecture. While this list is not complete, it will likely be expanded as the industry's experience with wireless clouds grows, as technologies evolve, and as the ingenuity of attackers seeks new ways to do so. achieve their goals. Knowing about threats is very useful for system administrators, testers, and information assurance professionals who need to understand how an information system can be attacked. The intention of a threat is to exploit a vulnerability of a weak point in an information system. In any risk assessment, threats must first be identified. For example, researchers such as [14] and [15] has identified some of the following threats against IEEE 802.11 WEP, the standard for wireless cloud networks, as follows:

A. Traffic Analysis

It is a simple technique whereby the attacker determines the load on the communication medium based on the number and size of transmitted packets, the source and destination of the packets, and the type of packets

B. Passive Eavesdropping

Passive attacker interception passively monitors the wireless session and the payload. If the payload is encrypted, this includes encryption violation to read clear text.

C. Active Eavesdropping

It involves the attacker injecting data into the communication to help decrypt the payload, then the attacker not only listens to the wireless connection, but actively injects messages into the communication medium to help determining the content of the messages.

D. Unauthorized Access

Unauthorized non-direct access to any user or group of users on the wireless local area network (WLAN). Once an attacker has access to the network, further attacks can be launched or free use of the network is provided.

E. Man-in-the-middle

It is to read the private data of a session or to modify packets violating the integrity of a session.

F. Session High-Jacking

An attack on the integrity of a session; the attacker steals an authorized and authenticated session from its owner.

G. Replay

It is use to access the network with target permissions, but the actual session(s) attacked are not altered or disrupted in any way. While many of the above-mentioned attacks are common in wireless environments, the high nature of wireless cloud deployment and collaboration will need to adopt enhanced security protocols to protect against threats originating from the wireless environment. wireless network, cloud environment, and cloud-transported data to network. As threats focus on specific attacks on cyber environments, the following model takes into consideration that threats should consider the ability of the attacker, his propensity to actually launch an attack, his concern about the risk of detection or attribution and the probability of success. The assumption is that the most skilled and motivated hackers would attack organizations deploying wireless cloud in their environment.

Threats to the Wireless Network Environment covers the conditions involved in the actual use of operational wireless network devices. Since each wireless network location connected to a cloud environment may be different, the worst environment should be considered from a risk assessment perspective. or bypass security functions within the wireless network. Threats from people gaining unauthorized physical or logical direct access to the security functions of wireless network devices and any alteration or misconfiguration could occur due to a threat to this environment. This also includes threats related to the theft or replacement of hardware or software devices that provide security functions within the wireless network. Threats that arise from the supplier's wireless network device supply chain for an organization can led to security issues in the wireless cloud architecture. The supply chain security challenges posed by the threat of attacks have important implications for businesses and their suppliers [16].

The whole process of implementing, maintaining, updating and patching hardware and software for wireless grid devices could introduce threats. Threats originating in the wireless network hardware/software device supply chain include those related to an adversary intentionally altering, bypassing or undermining security functions during development, production, distribution, maintenance, shipping and warehousing / storage of these entities. Since these functions are not perfect in their implementation, there is also the threat of an unintentional defect in the hardware or software of the device or in the security architecture of the overall wireless network in which they exist. Threats to a cloud computing environment are also of concern. There are several attack vectors within the software architecture of a cloud, including virtualization software, web browsers, security software, and client / server operating systems [17]. Attacks could also be launched against major cloud services, such as Amazon Web Services (AWS) and Google Apps, potentially affecting thousands of cloud consumers. (SOAP) and the Web Services Description Language (WSDL).

Supplier and consumer security services, such as anti-virus applications and personal firewalls, can be compromised. Attacks against web browsers can compromise communications between the consumer and the cloud provider and could allow attackers to intercept data (eg, passwords, encryption keys, files); redirect web browsers to compromised sites; and prevent the web browser from functioning properly, thereby inhibiting internet communications. One of the most critical and yet most difficult challenges is ensuring the continued availability of wireless cloud resources. Protection of critical infrastructure components, such as routers, gateways and the domain name system and DNS. The server and the communication paths between the cloud provider and the consumer are critical to maintaining the availability of resources as well as the integrity and confidentiality of the data transmitted through these channels. Threats affecting communications can be harmful, such as DoS attacks, targeting wireless connections or devices, vendors, consumers, or network resources; components of the authentication and encryption infrastructure; or unintentional outages, including technical failures, power outages, Internet congestion and natural disasters. Blacklisting Internet Protocol (IP) addresses used by consumers or cloud providers could also be a serious problem. Inappropriate behavior perceived by cloud consumers, originating from a data center of a cloud service provider, can result in blacklisting of the set of IP addresses used by the provider by the Internet service provider (ISP) and other cloud service providers.

Whether the actions were unintentional or harmful, blacklisting provider IPs would not only impact consumers' access to cloud services, but could also be financially devastating for a cloud provider. Physical security is about accessing the IT facilities, infrastructure, and personnel that support the cloud provider, consumer, and intermediate communication paths. While physical security is not unique to cloud computing, the shared resource environment of a wireless cloud architecture increases the potential for accessing data and computing resources in other organizations. A physical security breach within the cloud provider's data center allows intruders to potentially gain unauthorized access to the data of hundreds or thousands of users in various organizations [18].

Likewise, unauthorized access to computing resources in a consumer's facility can provide access to the cloud provider's environment, allowing the attacker to inject malware into the provider's infrastructure. Cloud provider administrators and maintenance personnel have physical access to shared cloud resources (e.g., hardware, power, network, storage, firewall). Threats associated with transporting data from the cloud to a wireless network environment should also be considered. The confidentiality and integrity of data must be protected at all times [19], whether the data is "at rest" or "in transit". The wireless cloud must provide protection against unauthorized modification of messages and documents during data transit. This is especially important in a wireless cloud environment, as cloud consumers will access data, applications, and services across the vast expanse of the Internet, thereby increasing the exposure of sensitive data to interception, modification and attack attacks. injection. Protecting data within the confines of a wireless cloud environment is just as important as public clouds are environments where compute resources are shared among potentially thousands of different users and must be protected from the prying eyes of other users. from the cloud.

It is also important to protect the underlying communication (transport) as well as the messages and documents that are carried during transport so that they cannot be made available to unauthorized persons. Typical threats to data in the wireless cloud can include unintentional or malicious tampering or deletion of data and files, data theft, and DoS attacks that prevent access to data, applications and services. The accidental alteration or deletion of data and files is often caused by improperly configured access controls against malicious attacks by hackers. Data in transit is susceptible to interception (for example, middle-class attacks), injection and modification, posing serious risks to data confidentiality and integrity. Data can be extracted without detection from misconfigured devices. Insufficiently protected end-user machines (such as at work or at home) can spread malware to a virtual machine (VM) and, in turn, spread to other users when they log into the VM.

When wireless cloud users connect to resources distributed across multiple virtual machines, malware can also spread. To reduce the potential spread of malware from personal or unauthorized devices, organizational security policies should determine whether security services, such as antivirus applications and personal firewalls, will be extended to protect personal computers. (PC), phones connected to the Internet or allow users to connect only to cloud resources with the computing resources provided by the company. Much like an outside hacker, an insider with authorized access to a wireless cloud system could perform various attacks to gain unauthorized access to other systems or deny service to users of those other systems and even manipulate information. files that facilitate the provision of services on virtual / remote machines. threat to wireless clouds

As businesses today face insider threats, the concentration of information and processing in wireless clouds will amplify the potential impact of insider information abuse. Wireless clouds will be particularly threatened by malware for two reasons: (1) The homogeneous structure, rich interconnections, and large scale of a cloud increase the possibility of an initial malware injection and may offer easy pathways. for the spread of malware. and (2) value concentration in a cloud offers potential attackers, both internal and external, a high-value target for bespoke and specialized malware projects. Wireless cloud data owners will need to be concerned about two potential threats: the accidental loss of information outside the security enclave and the negative impacts on the integrity or availability of their information due to the introduction of malicious code or DoS attacks. Wireless clouds will store and process information from a variety of sources (e.g., clouds, devices, etc.), provide access to many different users, and connect to a wide variety of external systems. This increases the risk of information loss between domains.

5.AUTHORIZATION

Once the user has demonstrated who is showing up, the next step is to give permission. Authorization is the granting of access to network resources and services and implies the limitation of internal resources by users; it also determines access control [20]. To provide full authentication function in the wireless cloud system, three categories of authorization sub-function must be implemented: establishment, operation and management. The first process is the constitution function; that is to say those relating to the correct start of the function and its correct operation. The second concerns operational functions, which are those that the authorization function performs to achieve its business purpose. The third category is the maintenance function, which is responsible for the proper functioning of the authorization.

The denial process should include provisions to identify malfunctions or failures in the mechanisms and resources of the function (for example, actions to repair, activate or terminate a free space or capacity, or a combination. or performance has occurred. has decreased below an acceptable level, management action, whether automated or human in cycle, must be initiated to resolve the problem. status, response status, and the like Values Performance monitoring monitors KPIs as specified in policies and reports or takes other action when performance degradation occurs, regardless of the cause. disposal is responsible for reporting status and updating, if necessary, a number of key values including criteria, CI, key materials, etc. this. ability to determine the impact of the compromise, identify options to mitigate the effect of the compromise, and select and execute the mitigation response option. The Metadata Provisioning feature initiates the discovery of the metadata schemas needed to assign valid metadata and discovery values from the messages generated by the authorization feature. The Report Accounting subfunction maintains usage logs showing when the authorization function is online and available, as well as transaction statistics and parameters.

Examples of these parameters include the number of request transactions, specific requests and transaction requests, the time the transaction occurred, and the time required before a response is initiated. Upon detection, this function will generate an audit log event record, which it will protect and archive internally. Based on another digital policy entry, it will report audit records. Finally, the backup system files create and store all the information necessary to restore or reset the working state of the authorization function. As with operational messages, the processing of output messages is responsible for determining the destination of a message and protect it according to the strategy (such as encryption, integrity protection, digitally sign it.

6.FUTURE SCOPE AND CONCLUSION

In this paper, we focus our discussion on security and authorization issues in the wireless cloud. The architectural perspective of the cloud targets various components of this architecture and protects them from security attacks. These components are the sensors, the cloud architecture and the channel that facilitates communication between the two entities. We expect security and privacy to be considered in the preliminary design phase of IoT systems to avoid the common drawback of seeing security as an afterthought. Although the pursuit of the position of smart objects is considered a violation of concealment; However, there may also be beneficial cases, for example, security agencies depend on tracking smart objects carried by a missing person to identify the location of the missing person. Such types of digital forensics in the IoT age will play an important role and should receive more attention in the future [21]. In addition, the domain of fog is expected to push computing capabilities to the edge of the network. In the future, we will pay more attention to this area as it has not received enough attention from academia and industry.

REFERENCES

[1] L. Lei, Z. Zhong, K. Zheng, J. Chen and H. Meng, "Challenges on wireless heterogeneous networks for mobile cloud computing," in IEEE Wireless Communications, vol. 20, no. 3, pp. 34-44, June 2013, doi: 10.1109/MWC.2013.6549281.

[2] https://searchcloudsecurity.techtarget.com/tip/Top-cloud-security-challenges-and-how-to-combat-them

[3] V. Carchiolo, A. Longheu, M. Malgeri, S. Ianniello, M. Marroccia and A. Randazzo. “Authentication and Authorization Issues in Mobile Cloud Computing: A Case Study.” In Proceedings of the 9th International Conference on Cloud Computing and Services Science (CLOSER 2019), pp. 249-256, doi: 10.5220/0007658602490256

[4] Z. Yin, F. R. Yu, S. Bu and Z. Han, "Joint Cloud and Wireless Networks Operations in Mobile Cloud Computing Environments With Telecom Operator Cloud," in IEEE Transactions on Wireless Communications, vol. 14, no. 7, 2015, pp. 4020-4033, doi: 10.1109/TWC.2015.2416177.

[5] https://researcher.watson.ibm.com/researcher/view_group.php?id=4171

[6] H. Lim, et al., “Automated Control in Cloud Computing: Challenges and Opportunities,” in Proceedings of the First workshop on Automated Control for Datacenters and Clouds (ACDC '09), 2009, pp. 13-18.

[7] G. Li, et al., “A Survey on Wireless Grids and Clouds,” in Proceedings of the Eighth IEEE International Conference on Grid and Cooperative Computing, 2009, pp.261- 267.

[8] Brooks, Tyson. (2012). In: Conceptualizing a Secure Wireless Cloud, International Journal of Cloud Computing and Services Science. 2012, pp. 89-114.

[9] CNSS Instruction 4009, “National Information Assurance Glossary,” Committee on National Security Systems, 2003, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[10] S. Jajodia, et al., In: Topological Analysis of Network Attack Vulnerability,” in Managing Cyber Threats: Issues, Approaches and Challenges, V. Kumar, J. Srivastava, A. Lazarevic (eds.), Kluwer Academic Publisher, Kluwer Academic Publisher, Chapter 5, 2003, pp. 248–266.

[11] S. Yi, et al., “Security-Aware Ad-Hoc Routing for Wireless Networks,” in Proceedings of the Second ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '01), 2001, pp. 299 – 302.

[12] P. Yau and C. Mitchell, “Security Vulnerabilities in Ad Hoc Networks,” in Proceedings of the Seventh International Symposium on Communication Theory and Applications (ISCTA’03) ,2003, pp. 99–104.

[13] C. Onwubiko and A. Lenaghan, “Managing Security Threats and Vulnerabilities for Small to Medium Enterprises,” in Proceedings of the 2007 IEEE International Conference on Intelligence and Security Informatics, 2007, pp. 244-249.

[14] D. Welch and S. Lathrop, “Wireless Security Threat Taxonomy,” in Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, 2003, pp. 76-83.

[15] H. Yang, et al., “Security in Mobile Ad Hoc Networks: Challenge and Solutions,” IEEE Wireless Communications, vol. (11)1, 2004, pp. 38-47.

[16] D. Closs and E. McGarrell, “Enhancing Security Throughout the Supply Chain. Michigan,” Michigan State University, IBM Center for Business of Government, 2004, pp. 1-52.

[17] H. Lohr, et al., “Enhancing Grid Security Using Trusted Virtualization,” in Autonomic and Trusted Computing, Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 2007, pp. 372–384.

[18] M. Armbrust, et al., “Above the Clouds: a Berkeley View of Cloud Computing,” Technical Report No. UCB/EECS-2009-28, Electrical Engineering and Computer Sciences, University of California at Berkeley, vol. 28, 2009.

[19] A. Raghunathan, et al. “Securing Wireless Data: System Architecture Challenges,” In Proceedings of the 15th International Symposium on System Synthesis (ISSS 2002), 2002, pp. 195-200.

[20] J. Chen and Y. Wang, “Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience,” IEEE Communications Magazine, vol. 43 (12), 2005, pp. 26 – 32.

[21] H. Johnson, et al., “SOLA: A One-Bit Identity Authentication Protocol for Access Control in IEEE 802.11,” in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'02), vol. 1, 2002, pp. 768- 772.