International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 04, No. 02, Feb-Mar 2024
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.42.11.18

Improved Digital Security Applications for Smart Card

Aseel Nadhum Kadhum*

**Computer Engineering, Digital Systems and Computer Electronics, College of Imam AL Kadhim (AS) Islamic Sciences, Babylon Branch, Iraq.*

*Corresponding Email: *Easeel18@yahoo.com*

Received: 28 September 2023 **Accepted:** 17 December 2023 **Published:** 01 February 2024

***Abstract:** With the rapid expansion of wireless networks and mobile computing applications, the quality of service (QoS) of mobile ad hoc networks (MANETs) has garnered growing attention. Ensuring QoS in a MANET system requires careful consideration of security issues. Attacks on a QoS distortion system without the protection of a security mechanism might result in subpar QoS performance, interference with resource use, or even failure of QoS provisioning. Traditional security measures cannot be applied because to the characteristics of MANET, which include limited processing and communication power and diversity of static topology. As a result, new security technologies are unavoidable. Nevertheless, not much research has been done on this subject. QoS and MANET system security are covered in this article. Consequently, the goal of this research is to create techniques for routinely evaluating security design reviews in order to make sure that all vulnerabilities, including security vulnerabilities, have been found, fixed, and their cause explained. Determine the system's fundamental security and protection needs by analyzing and determining its requirements. We create a network model using GloMoSim, specify node locations, communication features, and technology, and see if there are any vulnerabilities that could pose a security risk.*

***Keywords:** Security, Networking, IEEE, Bluetooth, AODV.*

1. INTRODUCTION

Radio waves are the most widely used transmission method in remote systems, where computers are connected and communicate with one another through a distinct electromagnetic dynamic flow. With a data transfer capacity of approximately 83 MHz, the accessible frequency response is arranged around the 2.4 GHz ISM (Industrial, Scientific and Medical) band; for a transfer speed of approximately 300 MHz divided into two sections, the 5 GHz U-NII (Unlicensed-National Information Infrastructure) band is used for remote transport. The suitable recurrence assignments are defined by regulations in the varied nations, comparable laws additionally direct the most extreme distributed transmission force, region (indoor, open air). The range of a remote radio station system like this is around 10-100 meters to kilometers, depending on the information, frequency, kind of receiving wire, and emission control. Omnis (omnidirectional radio wires), division receiving wires (directional reception devices), explanatory plates, and waveguide guides are only a few examples of the many forms of reception gear that can be used [1].

This infrared transit bolster caught my eye. Materials with haze are not susceptible to infrared light. The material is approximately ten meters long. Infaraed innovation is mainly utilized for little devices in WPANs (Wireless Personal Area Networks) for these kinds of applications, like linking a PDA to a tablet in the vicinity [1].

The major contributions of this research are:
(a) Security display design where information packages are randomly chosen and then encoded and unscrambled using different computations.
(b) Creating a security system's architecture to detect and thwart QoS threats.

2. RELATED WORKS

The study focuses on enhancing the smart card-based DRM authentication mechanism proposed by Yang et al. The plan attempts to generate session keys and enable mutual authentication within the DRM setting. Unfortunately, the researchers found that Yang et al.'s method lacked prior confidentiality, was vulnerable to smart card attacks, and did not have sufficient password update capability. The researchers propose an improved method that maintains security even if the user's smart card is misplaced in order to overcome these shortcomings. The user ID and password can be verified using their smart card technology. The research did not specify the precise context or situation in which the plan was evaluated. The suggested improvements may not be equally applicable or effective in all DRM settings or systems [13]. This study investigates the application of smart cards in the C-DAX project, which intends to develop an information and communication infrastructure for power distribution networks that is safe. The study shows that smart cards can hold long-term asymmetric keys and carry out cryptographic operations within the C-DAX infrastructure by developing and accessing several C-DAX security capabilities on a smart card. Although the research suggests a safe method for installing a smart card, other factors that need to be taken into consideration are key revocation, certificate systems, and the precise roles that the smart card and the consumer play [14]. The Multi-Elliptic Curve Cryptography (MECC) technique is the main tool used in this research to improve the security of encrypted smart cards. Unlike RSA, MECC offers better security with a smaller key size by utilizing numerous elliptical curves as opposed to a single curve. The outcomes demonstrate how successful this strategy is in providing enhanced security and minimizing picture distortion. It hasn't been thoroughly examined how scalable MECC-based encryption technology is. When working with huge volumes of data, it is crucial to confirm the performance and resource requirements of implementing MECC on smart cards. For upcoming security applications, the study recommends integrating Multi-Curve ECC technology into smart cards [15].

Standards

There by and by three primary gauges to remote systems: the IEEE 802.11 family, Hiper LAN, and, Bluetooth [2].

IEEE 802.22 Family

IEEE 802.11 is a standard released by the IEEE (Institute of Electrical and Electronics Engineers). From the motivation behind the physical layer, it describes three non-interoperable procedures: IEEE802.11 FHSS (Frequency Hopping Spread Spectrum) and IEEE 802.11 DSSS (Direct Sequence Spread Spectrum), which employs both the radio average at 2.4 GHz, and IEEE 802.22 IR (InfraRed). An expert data average of 1-2 Mbps is provided for a collection of different measurements.

IEEE 802.11a, also referred to as Wi-Fi, operates at 5 GHz U-NII strap using the OFDM (Orthogonal Frequency Division Multiplexing) transportation protocol and can handle up to Mbps of data at its highest. Because IEEE 802.11a and 802.11b use different frequencies, they are incompatible [2].

IEEE 802.11b, (Advertised WiFi), operating in the ISM band at 2.4 GHz. The information average, which depends on flag quality, is 1, 2, 5, or 11 Mbps. It is naturally balanced. The transportation route is determined by the information rate, which varies from 11 Mbps for 50 meters indoors (200 meters outside) to 1 Mbps for 150 meters indoors (500 meters outside). The transportation also follows the flag control [2].

I EEE 802.11g, at the 2.4 GHz band and support up to 20 Mbps of informational throughput. It makes use of both OFDM and DSSS in tandem to ensure conformance to the IEEE 802.11b standard.

IEEE 802.16, (presented as WiMAX), it was also aimed at WMANs (Wireless Metropolitan Area Networks) in this regard to overcome IEEE 802.11's range restrictions. It should provide organized coverage across a few square kilometers at frequencies ranging from 10 to 66 GHz. In order to address line-of-sight concerns when accessing the 10-66 GHz band, IEEE 802.16a, which operates in the 2-11 GHz range, was identified at the IEEE 802.16 standard [3].

Channel Get to Procedure: The inability to transmit and identify a transporter for parcel crashes in the interim is a crucial point in conduit get for systems to faraway systems. In this approach nothing true path to perform a CSMA/CD (Carrier Sense Multiple Access/Collision Detection) convention, for example, in wired Ethernet [3] [4].

HiperLAN

HiperLAN 1 provides a 10–20 Mbps information rate while using the 5 GHz frequency. HiperLAN 2 provides up to 54 Mbps of information transmission using the 5 MHz frequency. HiperLAN, a standard-related competitor of IEEE 802.16, aimed to provide range extension. It operates between 2 and 11 GHz [5].

Bluetooth

Bluetooth is standard composed by a consortium of privately owned corporations, for example, Agere, Ericsson. IBM, Intel, Microsoft, Motorola, Nokia and Toshiba. Bluetooth has a limited range of operation of about 10 meters and operates in the 2.4 GHz band using FHSS. Due to its low effort requirements, Bluetooth is appropriate for small WPANS and is also used for peripherals like consoles, printers, and mobile phone headsets. The Bluetooth is where Bluetooth radio invention operates. Reporters are organized into small units known as piconets, with an ace and one to seven dynamic slaves making up each piconet. A scatter net can be shaped by covering different piconets [6].

3. METHODOLOGY

There are several fundamental steps involved in designing a system for choosing QoS choices. An extensive analysis of the security system design for this purpose can be found below. [7] [8]:

To define requirements, we need to understand the specific requirements of the system, including the required level of quality of service, network privacy, and security measures. Define key performance indicators (KPIs) for QoS and security. We then perform a comprehensive analysis of potential threats and vulnerabilities that could affect QoS and harm network privacy. Identify areas of vulnerability in the system and potential attack vectors. We then assess the risks associated with the identified threats and vulnerabilities. And work to implement modern security measures, such as firewalls, intrusion detection systems, and encryption protocols, to protect the network and ensure privacy. Consider best practices and industry standards for security management.

Deploy monitoring systems to continuously monitor network activity and systems. Implement mechanisms for real-time detection of suspicious activities that may impact quality of service or network privacy. Define clear protocols for responding to detected threats or violations. Conduct comprehensive assessments, including functional and physical assessments, to ensure system effectiveness against potential threats and innovations, continuous improvement, documentation and training.

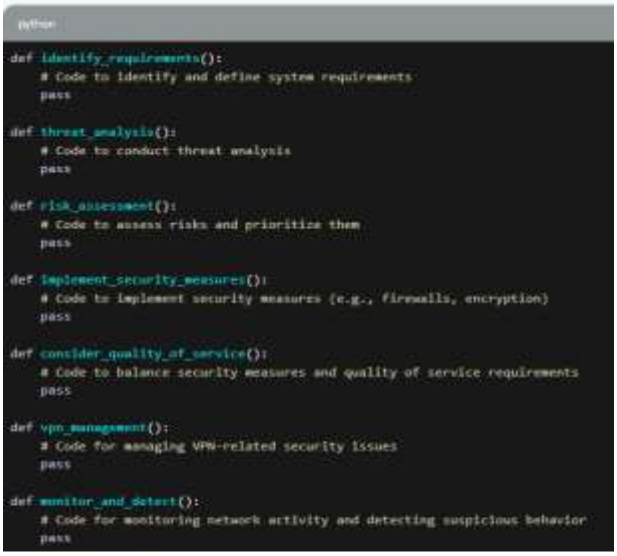
Finally, we customize this methodology to our specific system requirements and consider any industry-specific regulations or standards that may apply.

Performance Evaluation

The accompanying measurements were utilized to assess the execution of the information and defeat security. The accompanying measurements are assessed the productivity notwithstanding the adequacy of the conventions [9].

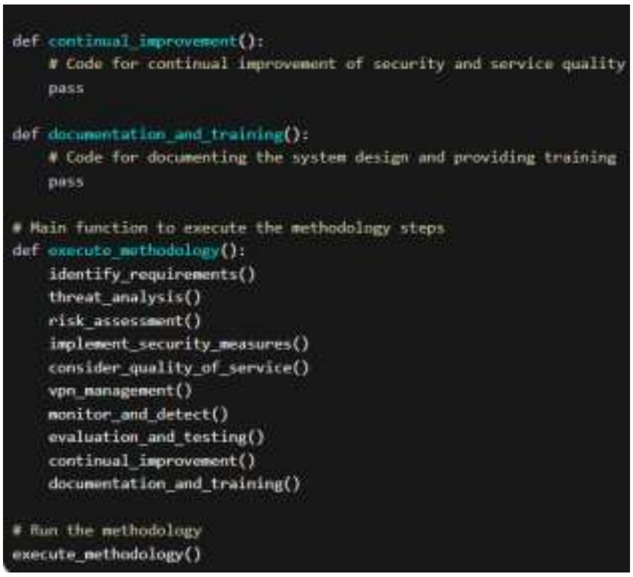
- Average performance, as used in security system architecture discussions, describes the efficiency with which data packets are managed and routed between specified sources and selected targets. A higher proportion of information packages transmitted between sources and recipients than information packages created by sources indicates high efficiency in direction and management [10].

- The packet throughput ratio calculates the effectiveness of sending packets from senders to recipients in relation to the amount of packets anticipated to be sent given the security system's general architecture. A high percentage means that the packet sending procedure is efficient, which in turn means that the security system's overall design is efficient [11].
- The term "end-to-end delay" describes the overall amount of time a message must spend traveling from its originating source to its intended location within the system. Put otherwise, it calculates the total amount of time couriers require to transmit from their location to their destination. This notion is crucial for assessing the effectiveness of the transfer process and guaranteeing that the system can operate at peak efficiency during the time frame [12].



```python
def identify_requirements():
    # Code to identify and define system requirements
    pass

def threat_analysis():
    # Code to conduct threat analysis
    pass

def risk_assessment():
    # Code to assess risks and prioritize them
    pass

def implement_security_measures():
    # Code to implement security measures (e.g., firewalls, encryption)
    pass

def consider_quality_of_service():
    # Code to balance security measures and quality of service requirements
    pass

def vpn_management():
    # Code for managing VPN-related security issues
    pass

def monitor_and_detect():
    # Code for monitoring network activity and detecting suspicious behavior
    pass
```

Fig. 1 Code the Methodology



```python
def continual_improvement():
    # Code for continual improvement of security and service quality
    pass

def documentation_and_training():
    # Code for documenting the system design and providing training
    pass

# Main function to execute the methodology steps
def execute_methodology():
    identify_requirements()
    threat_analysis()
    risk_assessment()
    implement_security_measures()
    consider_quality_of_service()
    vpn_management()
    monitor_and_detect()
    evaluation_and_testing()
    continual_improvement()
    documentation_and_training()

# Run the methodology
execute_methodology()
```

Fig. 2 Code the Methodology

4. SIMULATION RESULTS

The information security implementation can impact different values acquired with GloMoSim, as Figure 1 illustrates. Locking can result in changing data, varying speeds, and a varying number of axes. This average start-to-end delay vs node count is depicted in Figure 1.

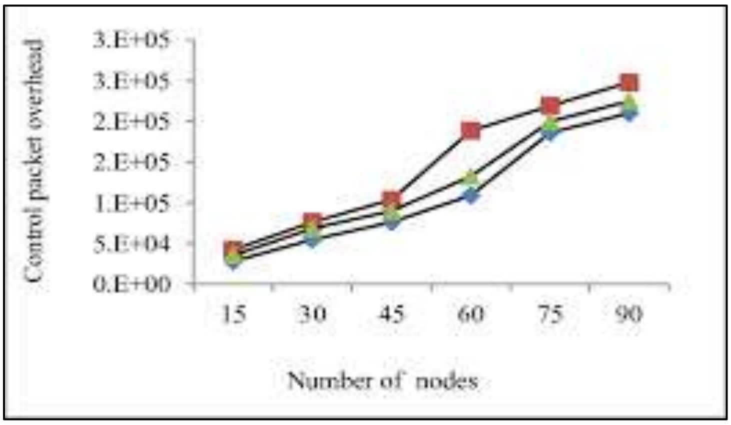


Fig. 1. Number of Control Packets Vs Number of Nodes Figure 2 examines public

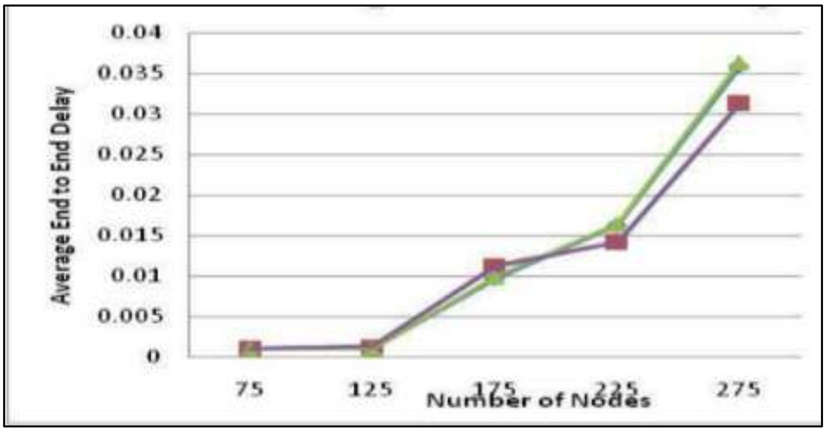


Fig.2. Average End-to-End Delay Vs Number of Nodes

Expenditure monitoring and how it relates to the number of axes operating at various speeds as well as the identification and tracking of systemic flaws. He also notes that by exiting the cycle, increases in control public spending can be increased. Figure 2 clearly shows that the expansion of multi-speed centers results in a small proportional increase in control public spending, which is primarily due to ongoing disappointments and the increasing brutality. In order to make sure that there are no abuses or infractions of specific laws and processes, these studies can be used to enhance security and monitoring policies inside government systems and businesses.

The Limitation

The attacker could access each and every sent path. If these requirements are met, there won't be much opportunity for reconstruction in terms of the smart card's information security. This includes the incapacity to build defenses against possible attackers trying to obtain access to broadcast channels and to improve security. The strictest requirements for data protection and smart card security must be followed in order to guarantee security in subsequent research. You can confirm that any relevant procedures and limits are followed correctly by checking with your card provider. It is also advisable to confirm that the private system architecture offers sufficient protection for the data being sent by reviewing internationally recognized security rules and requirements, such as PCI DSS standards.

5. CONCLUSIONS

Through the application of a novel approach that makes use of the random selection of cryptographic accounts on GloMoSim, the research seeks to enhance information security on mobile devices. The information security agreement's implementation and the training session with and without encryption were compared for results. Compared to unencrypted data, the results demonstrated a notable 80% improvement in data transfer rate. The study promotes secure course disclosure verification as a defense against security threats and dark vulnerability attacks. This research is significant from a security standpoint since it looks into fresh approaches to enhancing information security and aims to promote the adoption of safe course verification. From a technical point of view, the project aims to secure information and enhance the resilient and highly portable functionality of stacked systems.

6. REFERENCES

1. Umar, A., Mayes, K., & Markantonakis, K. (2015, February). Performance variation in host-based card emulation compared to a hardware security element. In 2015 First Conference on Mobile and Secure Services (MOBISECSERV) (pp. 1-6). IEEE.
2. Kaur, J., Kumar, A., & Bansal, M. (2017, September). Lightweight cipher algorithms for smart cards security: A survey and open challenges. In 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 541-546). IEEE.
3. Li, W., & Song, H. (2015). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE transactions on intelligent transportation systems, 17(4), 960-969.
4. Shuyao Yu, Youkun Zhang, Chuck Song and Kai, Chen,"A security architecture for Mobile Ad Hoc Networks ", Proc.
5. Azees, M., Vijayakumar, P., & Jegatha Deborah, L. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. IET Intelligent Transport Systems, 10(6), 379-388.
6. Winkler, T., & Rinner, B. (2014). Security and privacy protection in visual sensor networks: A survey. ACM Computing Surveys (CSUR), 47(1), 1-42.
7. Engoulou, R. G., Bellaïche, M., Pierre, S., & Quintero, A. (2014). VANET security surveys. Computer Communications, 44, 1-13.

8. Bariah, L., Shehada, D., Salahat, E., & Yeun, C. Y. (2015, September). Recent advances in VANET security: a survey. In 2015 IEEE 82nd vehicular technology conference (VTC2015-fall) (pp. 1-7). IEEE.
9. Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. Journal of network and computer applications, 37, 380-392.
10. Saini, M., Alelaiwi, A., & Saddik, A. E. (2015). How close are we to realizing a pragmatic VANET solution? A meta-survey. ACM Computing Surveys (CSUR), 48(2), 1-40.
11. Bariah, L., Shehada, D., Salahat, E., & Yeun, C. Y. (2015, September). Recent advances in VANET security: a survey. In 2015 IEEE 82nd vehicular technology conference (VTC2015-fall) (pp. 1-7). IEEE.
12. Rehman, S. U., Khan, M., Zia, T., & Zheng, L. (2013). Vehicular ad-hoc networks (VANETs): an overview and challenges. Journal of Wireless Networking and communications, 3(3), 29-38.
13. Kumari, S., Khan, M. K., & Li, X. (2016). A more secure digital rights management authentication scheme based on smart card. Multimedia Tools and Applications, 75, 1135-1158.
14. Baeten, M., Poll, E., & Vieira, B. (2014). Improving smart grid security using smart cards (Doctoral dissertation, Master's thesis, Radboud University Nijmegen, Faculty of Computer Science).
15. Prakash, G., & Sakthivel, S. (2014). Improving the security of smart cards through multi-curve ECC. International Journal of Applied Engineering Research, 9(22), 17601-17611.