ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

An Enhanced Framework for Secure Smart Parking Management Systems

Wafa A. Alkenazan[1], Ashraf A. Taha[2], Mohammed J.F. Alenazi[1], Wadood Abdul[1*]

[1] *Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, SAUDI ARABIA.*

[2] *Department of Computer Networks, Informatics Research Institute, the City of Scientific Research and Technological Applications, SRTA-CITY, EGYPT.*

**Corresponding Author (Email: aabdulwaheed @ksu.edu.sa).*

Paper ID: 12A7B

Volume 12 Issue 7

Received 04 February 2021
Received in revised form 12 April 2021
Accepted 23 April 2021
Available online 28 April 2021

Keywords:
ID card technology; Security attack; Smart parking; Performance of secure smart parking; Cryptography; Throughput with encryption, End-to-end delay; Data Encryption Standard (DES); Throughput without encryption; Secure hash algorithms (SHA); Smart parking under attack.

Abstract

The number of vehicles has increased significantly and it needs a smart parking system that helps users find an available parking space. Increasing car thefts are a cause of concern for users. Consequently, users attempt to find a secure parking spot. This paper focuses on achieving various aspects of security for a smart parking system. First, only authorized users can enter the secure parking lot. Each user has an identification card and a private complex password that is difficult to detect. Second, the national identification number, user name, and car plate number are encrypted using advanced 128-bit encryption algorithms. In addition, the user password is encrypted using secure 256-bit hash algorithms. In addition, we measure the performance of the proposed solution using the IEEE 802.11ac standard in terms of average end-to-end delay and throughput. Finally, we design an adaptive framework to model a smart parking system under attack with three scenarios. In the first scenario, if an attacker has access to the smart card and does not have access to the password. The second scenario, if ID card modification could be a threat to the system. The third scenario, when the parking ID number, ID card, and password are stolen by the attacker. The results present the encrypted case outperforms the unencrypted case in terms of the average end-to-end delay. In addition, in terms of throughput, we found that performance was better for the unencrypted case.

Disciplinary: Computer & Security Engineering, Cryptography.

Cite This Article:

Alkenazan, W. A., Taha, A. A., Alenazi, M. J. F., Abdul, W. (2021). An Enhanced Framework for Secure Smart Parking Management Systems. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 12*(7), 12A7B, 1-13. http://TUENGR.COM/V12/12A7B.pdf DOI: 10.14456/ITJEMAST.2021.128

1 Introduction

A smart parking system is a good example to illustrate how the Internet of Things is effective and efficient to make life easier [1]. Effective smart parking systems will optimize parking area usage by helping users to find a parking spot quickly. Recent studies have concluded that smart parking systems are necessary in all cities all over the world to reduce the impacts of such problems as air pollution, fuel consumption, and traffic congestion. Besides, the increasing number of car thefts makes users worry. Technical advances have improved security at parking spots.

Cryptography algorithms have been developed to protect data from malicious attacks. Cryptography converts plaintext into secret codes using a key and only authorized users can decode the message. Cryptography algorithms are used to protect data and communication by ensuring confidentiality, non-repudiation, and authorization. As shown in Figure 1, cryptography algorithms are classified as symmetric and asymmetric.

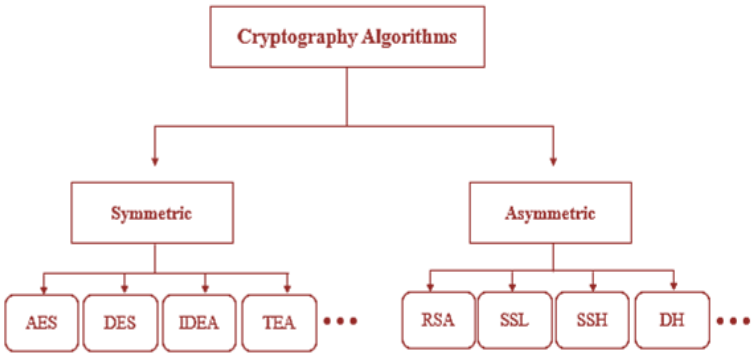

Figure 1: Cryptography algorithms.

Symmetric algorithms, i.e. secret-key cryptography, use the same key for encryption and decryption procedures. Various symmetric algorithms and encryption standards for symmetric algorithms have been developed, such as the Tiny Encryption Algorithm (TEA), the International Data Encryption Algorithm, the Advanced Encryption Standard (AES), and the Data Encryption Standard (DES) [2].

The DES was developed in 1974 by computer networking security scientists at the International Business Machines Corporation [3]. Symmetric algorithms involve two mechanisms, i.e. encryption and decryption. The original DES key length was 56 bits and encryption and decryption involved eight processes. The steps for decryption are the reverse of those for encryption.

The TEA is a symmetric algorithm created by David J. Wheeler and Roger M. Needham from Cambridge University in 1994 [4]. The 128-bit key is divided into four internal 32-bit keys. The TEA is based on the Feistel network with a block size of 64 bits with 32 rounds. The features of TEA are high speed and simplicity of implementation. It does not have S-Box and P-box.

Asymmetric algorithms, i.e. public key cryptography uses two keys, one for encryption and another for decryption. Some examples of asymmetric algorithms are Rivest Shamir Adleman (RSA), Secure Sockets Layer (SSL), Secure Shell (SSH), and Diffie-Hellman (DH) [2].

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described their algorithm in 1977 [5]. The RSA algorithm is a widely-used asymmetric algorithm that uses two keys; a public key and a private key. The public key is used to encrypt a message and it can be recognized by everyone. The private key is used to decrypt a message.

The SSH protocol enables a user to log into another computer over a network to execute commands and transfer files from one computer to another computer in a secure manner. SSH provides several security features, such as user authentication, host authentication, and knowledge integrity. The SSH protocol encrypts everything it transmits and receives. In addition, users can read, access, and edit files. Note that the SSH protocol does not improve security on a system that uses the Network File System (NFS) [6].

Diffie-Hellman is used to share secret key pairs for both encryption and decryption over unsecured channels. Only the two involved parties know the shared secret keys, even without having shared anything previously. Moreover, Diffie-Hellman is an asymmetric key algorithm. The Diffie-Hellman key length is short; therefore, computation is fast. Diffie-Hellman algorithms are vulnerable to denial of service and man-in-the-middle attacks. In addition, the sender and receiver are not required to be authenticated. The Diffie-Hellman algorithm is a secure key exchange algorithm [7].

To ensure secure communication between sensors connected to the cloud, we encrypt the data using 128-bit AES and 256-bit secure hash algorithms (SHA). AES algorithms are more secure, faster, and more efficient than other cryptography algorithms when properly implemented. In addition, they are simple to execute on a wide range of devices and are extendable to other key lengths [7, 8]. SHAs have a fast software implementation that ensures the hashing of the detected message authentication code (MAC) addresses without requiring a large buffer [9].

With the development of the Internet of Things [10], WSNs are becoming increasingly popular. Real-world applications of WSNs, such as smart parking, smart health, and smart farming could potentially require the deployment of thousands of sensors. In addition, this paper discusses IEEE802.11ac performance for secure smart parking to measure and analyze the average end-to-end delay and throughput. This performance analysis was done with and without encryption.

To improve the security of smart parking systems, our primary contributions are summarized as follows:

- To ensure that only authorized users can enter secure parking, an additional factor is required for authentication. Therefore, for MFA, each user has an identification card and a private password. The password should be complex (e.g. the password contains letters, numbers, and symbols) and difficult to guess.
- An advanced 128-bit encryption algorithm is used for the user's identification card and user passwords are encrypted using 256-bit SHAs.
- The performance of the system is evaluated using encrypted data and unencrypted data. Performance is measured using average end-to-end delay and throughput.

Attackers use technical expertise to achieve specific goals to create threats to disrupt systems. Therefore, an adaptive framework for modeling a smart parking system under attack with different scenarios is analyzed.

2 Related Works

This section presents the AES scheme and discusses the modeling that will be used. In addition, SHAs are described and several previous studies that investigated security in smart parking are reviewed.

Some studies have proposed improvements for security issues in smart parking systems, e.g., a privacy-preserving smart parking navigation system (P-SPAN) that integrates cloud storage and vehicle communication to provide secure smart parking navigation services for users has been proposed in [11]. This system uses a bloom filter (BF) and roadside units (RSU) to realize security. The BF is a probabilistic data structure used to determine if one element is a part of a given set. BF improves storage efficiency. RSUs communicate with each other and with the users. RSUs are connected to the Internet to communicate with the cloud. Also, the P-SPAN allows the cloud to guide a vehicle to free parking in real-time without revealing personal information about users. The users can access information in the cloud and retrieve encrypted navigation results by passing RSUs. BF reduces storage overhead and collision probability for RSUs to reach the privacy goal.

A secure and privacy-preserving framework for smart parking systems (SecSPS) has been proposed in [12]. This framework ensures the availability, integrity, and confidentiality of real-time information using two security mechanisms. The first mechanism is a secured communication channel that uses the Transport Layer Security (TLS) protocol. The primary goals of TLS are data integrity, authentication, and confidentiality. Here, data integrity is achieved using a Message Authentication Code (MAC). Confidentiality and authentication are achieved via a series of messages called a handshake. The second mechanism is the end-to-end encryption of application data. This process involves several components, e.g. parking lots with sensor nodes, smart gateways, brokers, and clients. The main goal of the sensor nodes is to monitor all parking spots to detect any presence of vehicles and calculate the number of free parking spots. The smart gateway receives the status of the parking lot from the sensor nodes and then analyses and encrypts the data. Then, the encrypted data are sent to the broker. The broker receives all encryption messages and determines who is interested in a message. Then, the broker sends the message to the client. Finally, the client, i.e. an electronic device, e.g. a smartphone or laptop that can connect to the broker.

A decentralized and privacy-preserving smart parking system using consortium blockchain has also been proposed in [13]. This system uses Private Information Retrieval (PIR) and Short Randomizable Signature (SRS). PIR is employed to maintain the privacy of the user's location and allows users to retrieve parking offers privately from blockchain nodes without revealing any information. The SRS is used for authentication and allows a user to reserve parking anonymously.

This system involves system initialization, submitting parking offers, parking offer retrieval, parking reservation, parking, and payment. During system initialization, anonymous credentials are created for users and an offline trusted authority generates public key certificates for parking spot owners. When submitting parking offers, all parking slots transmit their parking offers to blockchain nodes. In addition, parking offer recovery is performed when a user wants to retrieve the parking offers in a specific cell from specific blockchain nodes without revealing any information. This will allow the user to reserve parking in a specific cell. Finally, the parking and payment process is performed when the user arrives at the parking slot. Here, the parking fee is paid and the user with the reservation is authenticated.

A secure and smart parking monitoring, control and management solution (SPMS) based on the integration of ad hoc networks, RFID, IoT, and WSN has been proposed in [14]. This system model contains four layers, i.e. a sensor layer, a network layer, a middleware layer, and an application layer. In the sensor layer, a WSN using ultrasonic sensors detects and determines the status of parking spots, i.e. empty or occupied. The network layer collects data from different sensors and passes these data to the cloud. The middleware layer and application layer will provide the users with the status of parking in real-time. For computing is used to process and manipulate sensitive data at the edge of the network and increase response times in case of emergencies. Also, fog computing provides real-time information to detect parking spots and reservations.

A blockchain-based smart parking management system has also been proposed [15]. This system uses a consortium blockchain network and cloaking. Here, all parking offer transactions are processed and recorded in a consortium blockchain network. Cloaking techniques are employed to protect user location data. All parking spots submit their parking offers to the consortium blockchain network and then users transmit a transaction to the consortium blockchain network to retrieve parking offers in a cloaked cell to protect their privacy. Then, they select the most preferred offer. Finally, the parking fee is processed via Bitcoin to protect user privacy. This system involves two main phases, i.e. submitting parking offers and offer retrieval and reservation phases. In the submitting parking offers phase, parking spots transmit their parking offers to the blockchain network. In the offer retrieval and parking reservation phase, the user retrieves available parking offers in the desired cloaked cell from the blockchain and makes an online reservation.

A smart parking solution based on Raspberry Pi 3s devices and Bluetooth radio technology was developed for a small outdoor parking structure at George Mason University [16]. This solution includes a mesh network, central nodes, nodes, the Received Signal Strength Indication (RSSI), and Bluetooth Low Energy (BLE). The nodes form an authenticated network distributed over the parking slot's physical footprint. These nodes listen for broadcasts from a custom BLE beacon. The RSSI values from the broadcasts and the beacon hold by the nodes within range, encrypted, and sent back to a central node where space prediction occurs. The research uses the AES-128 algorithm with cipher block chaining mode and SHA-256 bit to encrypt messages. Every message

encrypts upon creation to maintain confidentiality and integrity. Each node receives two pairs of AES/SHA keys for use in broadcast messages that contain node management instructions from the central node. In addition, the central node specifies a unique identifier and the parking network's Bluetooth Universally Unique identifier to each node. Central nodes confirm the only nodes close enough to start a reliable connection joined to the network. Finally, a discovered node with consistent RSSI measurement less than 80 dBm is ignored and nodes with a measured RSSI of -80 dBm are authenticated.

A multi-factor authentication (MFA) system to ensure security in a smart parking system is proposed in [17]. This system uses a smart card and biometric data (fingerprint) and the smart card employs RFID technology. RFID contains information about the user and cannot change. In addition, the authors compared their system to an existing system. The existing system only uses RFID. They considered three scenarios: the first scenario, when a smart card is lost, someone other than the owner can use it. In the second scenario, if the smart card is cloned it should be considered a threat to the system. In the third scenario, if the smart card is rewritten, it should be considered a threat to the system. The researchers found that their system is very secure because the attackers fail to do any harm to the system.

3 Smart Parking Design

This section presents the architecture of the proposed secure smart parking system. The smart parking system is divided into two parts. When the users are registered, they go directly to a secure system. Other users must register using the registration system. In addition, this section describes the structure of the smart parking system and a model of the smart parking system under attack.

3.1 Secure Smart Parking Architecture

We achieve security in two ways, i.e., authentication and data integrity. Authentication allows only authorized users to enter the parking by comparing their identification to information in a database. If the information matches, the user is asked for their password, which is compared to the password stored in the database. To realize data integrity, we encrypt data using both AES and SHA. Figure 2 shows the registration diagram and Figure 3 shows the security diagram.

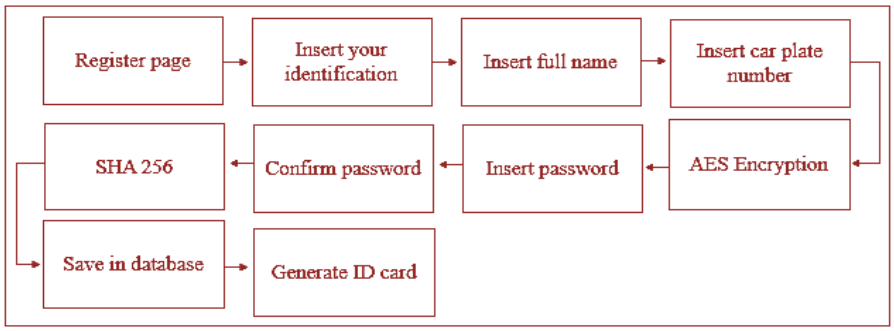

Figure 2: Registration process block diagram.

The following steps describe the registration process:

1. The user goes to the register page.

2. The user inserts their national identification, full name, and car plate number.
3. All information inserted by the user is encrypted using AES and then stored in the database.
4. The user inserts their password.
5. The password is encrypted by SHA and stored in the database.
6. Generate ID card parking that contains the encrypted national ID number, user name, and car plate number.

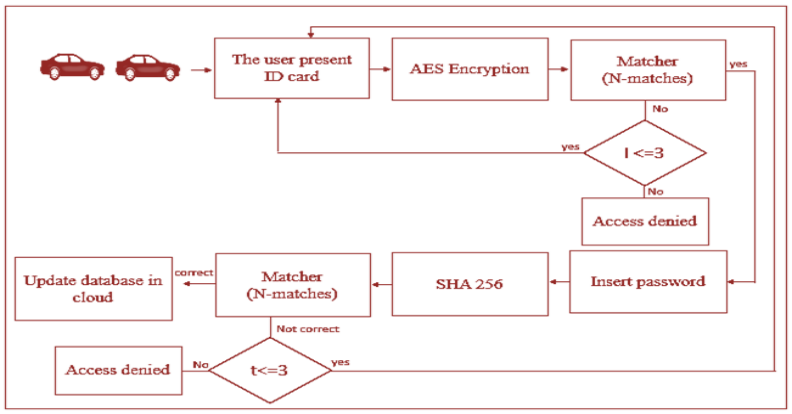

Figure 3: Secure system architecture.

The following steps describe the secure system architecture (authentication process):

1. Users outside the gate.
2. The ID card contains the user's national ID, user name, and car plate number. This information is encrypted and the parking ID number is not encrypted.
3. When the user inserts his/her card, the information is compared (user N-matches) to the information stored in the database. Here, two cases are considered.
    - The user is authorized.

The ID card number is compared. If this information matches the information in the database, the system encrypts the user's national ID, full name, and car plate number. The user is prompted to insert their password, which is encrypted by SHA. If the correct password is inserted, the user is permitted to enter the parking lot.

- The user is not authorized.

If the user is not authorized after three attempts, they are asked to register.

4. Two cases are considered when the user enters their password, which is encrypted by SHA.

4.1 Correct password

If the encrypted password matches the password stored in the database, the database is updated and the gate opens.

4.2 Incorrect password

If an incorrect password is input three times, the system will deny entry.

5. The database in the cloud is updated with user information and the status of parking.
6. The gate opens.

3.2 Structure of Parking

The parking design contains twenty-four parking lots. The area of the parking lot is 100x100 meters wireless sensors (magnetometers) that are placed under the ground surface to detect the presence of a car through variation in the electromagnetic field. Figure 4, shows the structure of the parking, where the black rectangle represents the parking while it is busy, white spaces are vacant park spots and red circles are magnetometers sensors. The encryption, hashing, and decryption of the user information are shown in different tables. Table 1 shows the encryption of user information, Table 2 shows user password encryption using SHA, and Table 3 shows the decryption of user information from the database.

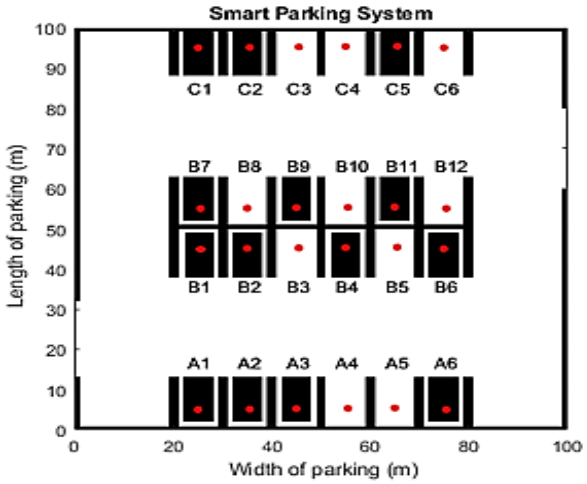

Figure 4: The parking structure.

Table 1: Encryption of user information.

parking ID number	5730
AES Encryption	
Identification number	1011778875
Ciphertext	òú#›¢K °¢âü-Þ
Full name	Tamim Tariq
Ciphertext	7Ü1Ï@=´ÀÆ„=>¶ÊP
Car plate number	def 5432
Ciphertext	|ÜÆ§™6}56÷r□ÖË

Table 2: The password encryption.

SHA Encryption	
The user password input	Aa_2017*
The password after hashing	'552D2EA858EAD0'0DB44FB4C10C68E3D30BAD9605D6555D62576AF3 B0B50412FE'

Table 3: Decryption of user information from the database.

The user inserts password:	**Aa_2017***
AES Decryption	
Ciphertext	òú#›¢K °¢âü-Þ
Identification number	1011778875
Ciphertext	7Ü1Ï@=´ÀÆ„=>¶ÊP
Full name	Tamim Tariq
Ciphertext	|ÜÆ§™6}56÷r□ÖË
Car plate number	def 5432

When the user inserts an ID parking number, ID card then the system will encryption his ID national number, user name, and car plate number as shown in Table 1. Then the system asks him to insert his password, if the password is correct, the data is decrypted and the user information is retrieved as shown in Table 3. If the password is incorrect, the parking prints a message telling him that he is not authorized to enter the parking. For example, when a user at parking spot C5 is ready to leave his parking, then he must insert his password to leave the parking. When the user inserts his password, the system encrypts and verifies his data, as shown in Table 2. Finally, the gate of parking is opened and the user leaves the parking lot as shown in Figure 5. Then the database is updated.

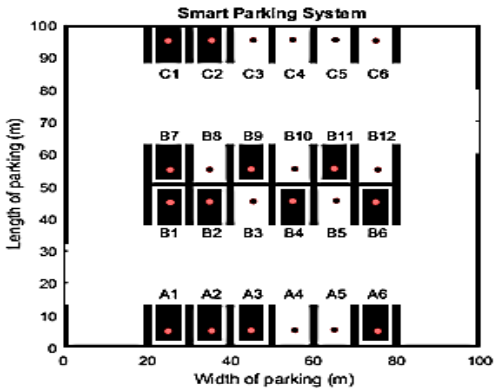

Figure 5: When the user leaves C5 parking.

4 Modelling Smart Parking under Attack

To secure the system, several attacks that can occur in the smart parking authentication system were evaluated. Some of the attacks and scenarios that can appear in smart parking authentication are summarized as follows.

A. The attacker has access to the smart card and he does not have access to the password.

B. ID card modification could be a threat to the system.

C. The parking ID, ID card, and password are stolen by the attacker.

4.1 Attacker Uses an Incorrect Password to Enter the Smart Parking Lot

The attacker tries to pass the authentication system with an authenticated identification card. Then, they insert the parking ID number and, if it is correct, the system verifies the identification card and asks the user to enter their password to complete authentication. If the password is incorrect (the attacker does not have the password), authentication fails and the attacker cannot enter the parking lot. This scenario is shown in Figure 6.

4.2 An Attacker Uses a Modified ID Card to Enter the Smart Parking Lot

Here, an attacker passes the authentication system using a correct parking ID number with a modified ID card. Then, the system identifies that an attacker is trying to access the parking. The system identifies that the ID card has been modified. Therefore, authentication fails and the attacker cannot enter the parking. This testing scheme is shown in Figure 7.

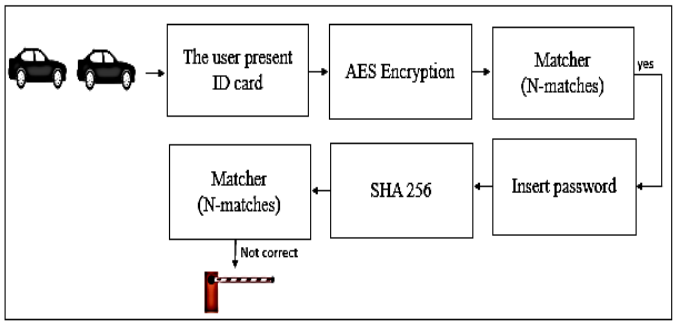

Figure 6: The incorrect password scenario.

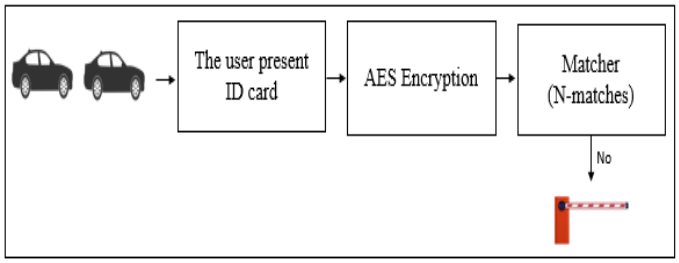

Figure 7: Incorrect identification scenario.

4.2.1 Using an Authenticated ID Card and Password to Enter the Smart Parking Lot

The user has passed the authentication system with the parking ID number and an authenticated ID card. Then, the system authenticates the identification card. If the ID card matches the information in the database, the user is prompted to enter their password to complete authentication. In this scenario, the user enters the correct password. The expected result is successful authentication and an attacker has gained access to the parking system. This testing scheme is shown in Figure 8.

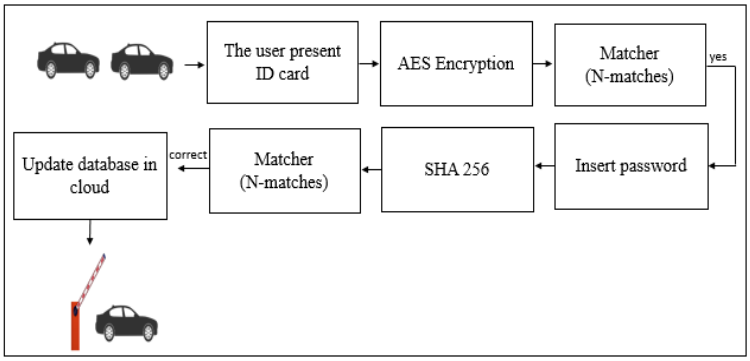

Figure 8: Authentication scenario.

5 Performance of Secure Smart Parking

We distributed a hundred sensors in grid placement. We measure the performance of IEEE802.11ac by using a scenario with encryption and another scenario without encryption to analyze the average end-to-end delay and throughput. The measured average end-to-end delay and throughput results are shown in Figures 9 and 10 respectively. The average end-to-end delay was calculated using Equation 1 [18, 19].

$$Average\ end\ to\ end\ delay = \text{transmission delay} + \text{propagation delay} + \text{queuing delay} + \text{processing delay} \quad (1),$$

$$Transmission\ delay = \frac{Packet\ length}{Link\ bandwidth} \quad (2),$$

$$Propagation\ delay = \frac{Length\ of\ physical\ link}{Propagation\ speed\ in\ medium} \quad (3).$$

Where, transmission delay (d_trans) is the time taken to transmit the data, propagation delay(d_prop) is the time required to send a single bit from the sender to the receiver, queuing delay (d_Queuing) is the duration a data packet sits in a queue before execution and processing

delay (d_process) is the time required by the system to execute the data packet. Throughput means how much data can be transferred from one position to another in a given amount of time, it is represented by [20]

$$Throughput = \frac{Transfer\ size}{Transfer\ time} \quad (4).$$

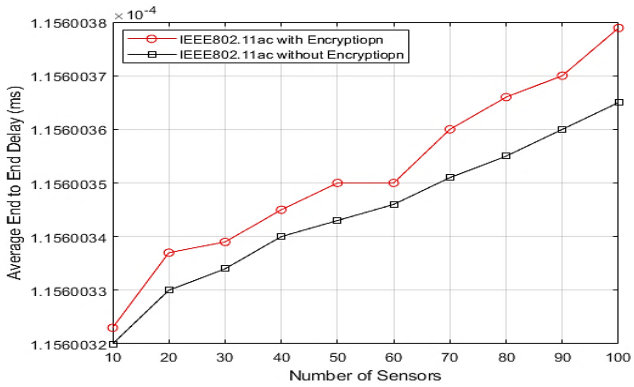

Figure 9: Average end-to-end delay with and without encryption.

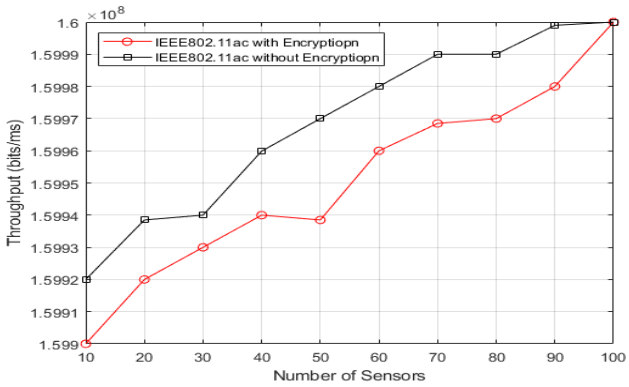

Figure 10: Throughput with and without encryption.

As shown in Figure 9, the average end-to-end delay with and without data encryption is close and this means that the performance of the system is only slightly impacted due to the encryption process. As expected, the average end-to-end delay increases for both cases when the number of sensors is increased.

Figure 10 shows the throughput measurements with and without data encryption. It demonstrates that the performance in terms of throughput is better without encryption. In addition, Figure 10 shows that throughput increases with an increase in the number of sensors.

When using parameters of average end-to-end delay and throughput while considering the encrypted and unencrypted scenarios, the following conclusions are drawn:

- The average end-to-end delay is increased when the number of sensors is increased.
- The average end-to-end delay is slightly better in the case when the data is unencrypted. This means that the proposed smart parking security approach is effective and does not impact the performance in a negative way.
- The throughput of the scenario without encryption is also slightly better than the scenario with encryption.

6 Conclusion

In this paper, we have presented a secure parking system that uses ID card technology. The security feature of the system employs a password that is required to enter and exit the parking lot. From the obtained results, we conclude that the proposed system enhances vehicle safety in parking lots. In addition, we measured the average end-to-end delay and throughput with and without encryption. We found that the encrypted case outperforms the unencrypted case in terms of the average end-to-end delay. In addition, in terms of throughput, we found that performance was better for the unencrypted case.

7 Availability of Data and Material

Information is available upon request to the corresponding author.

8 References

[1] J. Cynthia, C. Priya, and P. Gopinath, "IOT based smart parking management system", International Journal of Recent Technology & Engineering, vol.7(4), pp.374-379, 2018.

[2] T. Guy-Cedric, and R. Suchithra, "A Comparative study on AES 128 bit and AES 256 bit", International Journal of Scientific Research in Computer Science, vol.6(4), pp.30-33, 2018.

[3] R. A. Ratnadewi, Y. Hutama, A. Ahmar, and M. Setiawan, "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in a communication system based near field communication (NFC) ", Journal of Phys. Conference Ser., vol.954, 2018.

[4] M. Novelan, A. Husein, M. Harahap, and S. Aisyah, "SMS security system on mobile devices using tiny encryption algorithm", IOP Conf. Ser. J. Phys. Conf. Ser., vol.1007, 2018.

[5] S. Sharma, and Y. Gupta, "Study on cryptography and techniques", International Journal of Scientific Research in Computer Science, Engineering & IT, vol.2(1), pp.249-252, 2017.

[6] K. Sivaraman, "A research on secure shell (SSH) protocol", International Journal of Pure and Applied Mathematics, vol.116(8), pp.241-246, 2017.

[7] J. Athena, and V. Sumathy, "Survey on public-key cryptography scheme for securing data in cloud computing", Circuits and Systems, vol.8(3), pp.77-92, 2017.

[8] L. Thulasimani, and M. Madheswaran, "A single-chip design and implementation of AES -128/192/256 encryption algorithms", International Journal of Engineering Science & Technology, vol.2(5), pp.1052-1059, 2010.

[9] A. Boubrima, W. Bechkit, and H. Rivano, "Optimal WSN deployment models for air pollution monitoring", IEEE Transactions on Wireless Communications, Institute of Electrical and Electronics Engineers, vol.16(5), pp.2723-2735, 2017.

[10] M. Collotta, G. Pau, T. Talty, and O. Tonguz, "Bluetooth 5: a concrete step forward towards the IoT", IEEE Communications Magazine, vol.56(7), pp.125-131, 2018.

[11] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval", IEEE Transactions on Vehicular Technology, vol.67(7), pp.6504-6517, 2018.

[12] A. Alqazzaz, I. Alrashdi, E. Aloufi, M. Zohdy, and H. Ming, "Secsps: A secure and privacy-preserving framework for smart parking systems", Journal of Information & Security, vol.9(4), pp.299-314, 2018.

[13] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Privacy-preserving smart parking system using blockchain and private information retrieval", In 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), pp.1-6, 2019.

[14] O. Abdulkader, A. Bamhdi, V. Thayananthan, K. Jambi, and M. Alrasheedi, "A novel and secure smart parking management system (SPMS) based on an integration of WSN, RFID, and IoT", Learning and Technology Conference (L&T), pp.102-106, 2018.

[15] W. Al Amiri, M. Baza, K. Banawan, M. Mahmoud, W. Alasmary, and K. Akkaya, "Towards secure smart parking system using blockchain technology", In 2020 IEEE 17th Annual Consumer

Communications and Networking Conference (CCNC), pp.1-2, 2020.

[16] P. Seymer, D. Wijesekera, and C. Kan, "Secure outdoor smart parking using dual-mode Bluetooth mesh networks", In 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pp.1-7, 2019.

[17] I. Insan, P. Sukarno, and R. Yasirandi, "Multi-factor authentication using a smart card and fingerprint (case study: parking gate) ", Journal of Computing, vol.4(2), pp.55-66, 2019.

[18] B. Forouzan, and S. Fegan, "Data communications and networking", 4th Ed., New York, Alaan r.apt, pp.90-92, 2007.

[19] J. Kurose, and K. Ross, "Cooper networking -a top-down approach", 2013.

[20] S. Singh, and S. Prasad, "Techniques and challenges of face recognition: a critical review", Procedia computer science, vol.143, pp.536-543, 2018.

Wafa Abdulaziz Alkenazan received a B.S. degree in Networking and Telecommunication Systems from the Princess Nourah bint Abdulrahman University, Saudi Arabia., an M.S. degree in Computer Engineering from King Saud University, Saudi Arabia. Her research encompasses Wireless Sensor Networks, the Internet of Things, Privacy, Biometrics, and Security Networks.

Dr.Ashraf Abdelaziz Taha is a Researcher at the Department of Computer Networks, the City of Scientific Research and Technological Applications (SRTA City), Egypt. He got a B.S. degree in Electronics Engineering from Menoufia University, Egypt, an M.Sc. degree in Computer Science and Engineering, from Menoufia University, Egypt, and a Ph.D. degree in Electrical Engineering from Alexandria University, Egypt. He was an Assistant Professor in the Department of Computer Engineering, King Saud University (KSU). He earned STDF Visiting Grants in the Speed School of Engineering, Department of Computer Engineering and Computer Science (CECS), Louisville University, Kentucky, USA. His research interests are Video Streaming over Networks, the Internet of Things, and Wireless Communications and Networking communication.

Dr.Mohammed J.F. Alenazi is an Associate Professor of Computer Engineering at King Saud University. He received his B.S. and M.S. degrees in Computer Engineering from the University of Kansas and a Ph.D. in Computer Science from the University of Kansas. His research interests encompass Design, Implementation, and Analysis of Resilient and Survivable Networks, Network Routing Design and Implementation, Development and Simulation of Network Architectures and Protocols, Performance Evaluation of Communication Networks, Algorithmic Graph Approach for Modeling Networks, and Mobile Ad Hoc Networks (MANET) Routing Protocols. He is a senior member of the IEEE and a member of the ACM.

Dr. Wadood Abdul is an Associate Professor in the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University. He got his Ph.D. in Signal and Image Processing from the University of Poitiers, France. His research interests focus on Multimedia Security, Biometrics, Agriculture Applications, Privacy, Medical image Processing, and Video Understanding. He developed the Communications Laboratory by Lucus Nulle and the Biometrics Laboratory funded by ZKTeco at King Saud University. He received the Best Faculty Award from the College of Computer and Information Sciences, King Saud University, in 2017.