

RESEARCH ARTICLE

PufParkChain: Secure and Smart Parking Based on PUF Authentication and Lightweight Blockchain

MARIEM TURKI^{1,2}, BOUTHAINA DAMMAK³, AND AMNAH ALSHAHRANI³

¹ISIMG, Gabes University, Gabes 6033, Tunisia

²CES Laboratory, University of Sfax, Sfax 3038, Tunisia

³Department of Computer Science, Applied College, Princess Nourah Bint Abdulrahman University, Riyadh 11564, Saudi Arabia

Corresponding author: Bouthaina Dammak (Badammak@pnu.edu.sa)

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number RI-44-077.

ABSTRACT Smart Parking Systems have emerged as a transformative solution to address the growing challenges associated with urbanization and increasing vehicular traffic. Such system integrates sensors, cameras, and other IoT connected devices to monitor parking spaces in real time. However, there are many security vulnerabilities in existing solutions, especially when it comes to car authentication at parking entry points. IoT sensors may be susceptible to Cyber-attacks and fraudulent activities, such as car theft, can exploit these vulnerabilities due to limited built-in security features. The reliability of authentication systems, based on IoT sensors can also be compromised by factors such as extreme weather conditions and physical damage. The cyber-physical solution we propose relies on Physical Unclonable Functions (PUFs) for identification and authentication in IoT devices to mitigate these challenges. The use of PUFs enhances the reliability and security of smart parking systems against unauthorized access and fraud. Furthermore, to ensure the integrity and confidentiality of the data within the smart parking ecosystem and to improve authentication process, we propose the implementation of a tailored blockchain framework. This framework incorporates lightweight local blockchains dedicated to individual parking slots, complemented by a central blockchain that manages data at the city level. The experimental results demonstrate the feasibility of the PUF computation process, showcasing an acceptable runtime for practical implementation. In the experimental results, we evaluated the SRAM used for the PUF implementation process and demonstrated its stability (intra HD equals to 2.25).

INDEX TERMS Internet of things, lightweight blockchain, PUF, smart parking system.

I. INTRODUCTION

Over half of the world's population already resides in metropolitan areas, with estimates showing future development in both size and population. Consequently, the significance of efficient urban management cannot be overstated. According to the UN World Urbanization Prospects, over 66% of the world's population is projected to reside in cities by 2050 [34]. Despite occupying just 2% of Earth's surface, cities use up 75% of the resources on Earth [35]. This emphasizes how important they are to sustainable development. This paper seeks to shed light on a specific facet

The associate editor coordinating the review of this manuscript and approving it for publication was Rakesh Matam¹.

of urban innovation – smart parking systems. Smart parking, serving as a microcosm of smart urban solutions, provides an insightful case study that encapsulates the broader principles of efficiency, sustainability, and improved citizen welfare.

The demand for smart parking systems stems predominantly from two issues [3]. The increase in the number of vehicles in metropolitan area, along with the lack of management of available parking spaces have the problem of illegal parking on the side of roads [12], [33]. Moreover, every day, one million barrels of the world's oil supply are used up in the search for parking spaces which further trails to an increase in air pollution. If the search for parking spaces was reduced or eliminated, citizens quality of life (QoL) would be improved.

Modern cities increasingly employ IoT-based systems for monitoring purposes, including parking [8]. These systems involve wireless sensors in parking spots to continuously collect the number of available parking spaces in a given parking facility or area. This data is collected and updated by wireless sensors installed in individual parking spots [16], [41]. This information is transmitted via wireless networks to a cloud platform for processing and storage. A connected mobile app notifies users of nearby parking spots. Additionally, research efforts have been conducted to address real-time track of free parking slots and provide ability to booking [4], [15].

Despite the many benefits of Smart Parking Systems, they face communication challenges related to security, privacy, and single-point failures. Cloud servers operating through wireless networks are susceptible to online threats. Single-point operational failures can disrupt the system, leaving drivers unable to find parking spaces, a problem exacerbated by the growing data volume. Private parking owners also grapple with issues regarding data sharing and ownership after leasing contracts expire, which can lead to concerns about trust and privacy. This problem highlights the need for blockchain technology in ensuring secure and transparent data management in such scenarios. Additionally, the parking system should be enhanced with a robust reporting mechanism for illegally parked vehicles in order to facilitate more efficient urban mobility while promoting a safer and more orderly environment.

In this context, the advent of blockchain technology combined with IoT devices and cyber-physical systems that collect and exchange data could offer a promising solution [19].

Blockchain, serving as a decentralized ledger system, it ensures data immutability and enhances transparency. Blockchain also reinforces trust measures for Internet of Things (IoT) devices [13], [38], applications, and cyber-physical systems by eliminating the need for a reliable third party. Physical Unclonable Functions (PUFs) are considered as a cyber-physical mechanism in IoT systems through the generation of a unique key based on physical properties of the electronic device [7]. The unique physical characteristic enables IoT networks to authenticate devices and communicate securely.

Nonetheless, blockchain systems are resource-intensive and need significant processing power and communication resources, which can inhibit IoT devices to respond timely especially if they are full blockchain nodes. Consequently, a need arises for a solution that enables IoT devices to engage with the blockchain network while preserving their limited resources. Recently, the concept of a local blockchain has emerged to address this issue in the context of Healthcare systems. To address similar challenges within the context of parking systems, we adopt the concept of a local blockchain as proposed by [11].

In this approach, we introduce an innovative parking system PufParkChain, a decentralized Internet of Things (IoT)

application that combines blockchain and PUF technologies. PufParkChain guarantees cyber-physical security and integrity of the data of vehicles entering parking lots. Based on PUF, The proposed approach ensures that the authentication as well as the timestamp linked with a registered vehicle's entry cannot be altered, deleted, compromised, or called into doubt as to its accuracy. Moreover, PufParkChain includes a blockchain structure composed of local blockchains for each parking slot, coupled with a global blockchain situated at the cloud layer (dedicated to smart city level). For each parking slot, block headers of all blockchain blocks are preserved, along with the bodies of the blocks relevant to the local chain, and the essential smart contract functions required for local operations. In contrast, the global blockchain encompasses complete blocks and the entirety of smart contracts. Hence, we explore the concept of local and main blockchains, which can enhance traceability and enable comprehensive data analysis at the city level by aggregating data from various parking clusters/slots. The local blockchain within each parking cluster can maintain data integrity and security for localized operations, while the main blockchain at the city level can facilitate holistic data analysis and decision-making. This approach allows for a more efficient and effective management of smart parking resources and traffic flow throughout the city.

The contributions of this paper are manifold.

- To allow tracking all vehicles' access in real-time through recording all the data on a decentralized ledger for greater traceability.
- To shed light on the expansive capabilities of blockchain technology to be leveraged in different aspects of cyber-security across diverse domains. These include authentication, identification, and authorization.
- Smart Parking system identifies illegally parked vehicles and promptly notifies relevant public authorities about traffic safety violations.
- The blockchain network is composed of full nodes, which constitute the main blockchain where all blocks are stored, as well as a collection of lightweight nodes forming local blockchains in each parking cluster for quick access during authentication and optimized resource management.
- To the best of our knowledge, this research represents the pioneering work in introducing the concept of employing Physical Unclonable Function (PUF) keys for vehicle authentication within the context of smart parking systems. This innovative approach marks a significant advancement in the field, offering a novel and robust method for vehicle authentication.

The paper's structure is as follows: Section II explores related works concerning previous parking solutions, providing a comprehensive overview of the existing landscape. Section III offers a holistic view of the proposed architecture and its components, setting the stage for a thorough understanding of the innovative system. Section IV delves deep into the interactions among these components, especially the

PuF mechanism and the lightweight blockchain network which are the main contributions of the PufParkChain system. Section V provides detailed insights into the technical implementation, accompanied by a comprehensive security analysis of the PufParkChain, emphasizing its robustness and safety measures. Finally, Section VI concludes the paper, summarizing key findings and contributions, and offers a glimpse into potential future endeavors and developments in this field.

II. RELATED WORKS

Smart parking solutions for the market and smart cities are expanding rapidly using an architectural framework that contains different application platforms integrated into embedded systems [10]. The use of IoT technology to monitor and manage the parking system is in expansion.

A. SMART PARKING SYSTEMS BASED ON IOT

In [27], [28] [20], and [29], we find prototypes of smart parking systems based on IoT devices such GPS sensor, ultrasonic sensors and Raspberry Pi Microcontroller that gathers and upload data to the server via Wi-Fi. In [27], Lookmuang et al. enhance their system with computer vision to detect the car's plate and locate the vehicle whenever the driver forgets the parking location. The payment is also enabled through the mobile application. In [5], the authors propose a similar parking system that integrates IoT technology along with RFID, WSN and NFC. Their solution helps user to easily look for nearby parking lots alongside real-time availability in each parking lot. They can also block the desired parking slot through the app, followed by reaching the parking lot and authenticating using an RFID tag. In citeICCC2016, the authors propose an architecture which brings IoT gadget including sensors and microcontrollers along with TCP/IP protocol for exchanging parking data. More recently, the use of IoT devices and sensors is also found in [36]. The authors propose a system based on a Raspberry-Pi that activates a servo motor to take a picture of the car's plate. A CNN model is used to increase cars recognition accuracy and improve the estimation of parking demand. Also, in [1], the authors propose to use CNN model to suggest for drivers a number of parking spots that are useful in making a decision on where to park. Moreover, there system is enhanced by face recognition process to make a secure authentications on parking slots. Such system may use confidential data to operate, which make parking and vehicle honors reluctant to use such systems. Recently, some works proposed the use of blockchain technology combined with IoT devices to design secure smart parking systems [22]

B. SMART PARKING SYSTEMS BASED ON IOT AND BLOCKCHAIN

Ahmed et al. [6] standardized a framework for blockchain-based smart parking Systems. They integrate a transaction layer which is responsible of transactions between the network node and provides the consensus of the blockchain.

In [18], the authors propose a blockchain-based smart parking solution integrating smart contracts to establish legal and financial transparency between the different actors. Their solution proposes the exploitation of unused lands by a lease contract between the owner and other participating parties. They employ Non-Fungible token (NFT) [31] to create digital assets for unused lands and set up a smart parking pool. In [23], Kim and Kim propose a parking system integrating Mobile crowdsensing (MCS) technology [26] and Multi-blockchain structure. The proposed system rely on MCS that consists on collecting sensing data from users who contribute with their mobile devices as basic sensing units. The contributors can access to the public Ethereum Blockchain to provide sensing data related to free parking slots. In [37], the authors propose BRP, a parking reservation framework based on blockchain and integrates a reputation mechanism [14] to manage vehicles behaviour and reduce the number of malicious nodes and resulting in wasted parking spaces. Their solution integrates also deep learning (DL) to adjust dynamically the size of Hyperledger blocks and make the blockchain running more efficiently. In [32], the authors propose the use of XNO, which is a digital currency as a way to keep track of available parking spaces via IoT nodes. IoT devices are at entry and exit points of the parking and uses ultrasound sensors that detect the approaching objects and maintain appropriate XNO balance securely stored on a blockchain network In [2], the authors propose a smart parking that uses a decentralized local server as a fog node to deliver fast data exchange for parking information.

C. ANALYSIS

Many advancements in parking systems using computer vision [1], [36], RFID tags [5], [28], deep learning [1], [36] and Blockchain-IoT integration [32], [37] [6], [31] [23] have mitigated many parking issues namely time saving, management of parking places and traffic congestion alleviation. Hence, there is still a need to improve these systems. The listed works rely on IoT devices integrated along with RFID tags [5], [28], Ultrasonic sensors [23] or cameras [1], [36] to authenticate a car in a parking slot through its plate. Their solutions may be susceptible to security issues or cyber-attacks during car authentication on parking entry due to their limited built-in security features. The car plate can be changed and the parking entry database may not be effective in assisting authorities in critical situations such as car theft. Moreover, such authentication systems may be exposed to harsh weather conditions, temperature fluctuations, or physical damage, affecting their reliability. To address this, our solution employs a cyber-physical solution based on PUF as a hardware solution for identification and authentication in IoT devices. Moreover, Blockchain-based IoT smart parking smart parking systems face challenges related to blockchain requirements in terms of computation and processing resources. These

challenges can limit the system's time efficiency. In our work, the blockchain network is constituted of local blockchains specialized for each parking slot, coupled with central blockchain. This approach allows an effective management of parking Systems through the city.

III. PUF-PARKCHAIN ARCHITECTURE OVERVIEW

In this section we give a general overview about the Puf-ParkChain solution poised to revolutionize parking allocation systems. As shown in Figure 1, this architecture comprises a multitude of interconnected components, each playing a crucial role in ensuring the seamless operation of the PufParkChain.

A. PARKING SLOTS

The main component within the proposed solution is the parking building housing multiple slots. The parking should be suitably arranged to streamline the entry and exit process. Moreover, the access area must be strategically positioned for easy navigation, minimizing congestion and optimizing traffic flow in and out of the parking facility. Parking facilities can fall into two main categories: private, like residential parking, or public, such as employee parking.

B. SMART INFRASTRUCTURE

The parking slot access is controlled by a Smart Access Control System (SCAS). This system encompasses a smart technology to manage and regulate the entry and exit of vehicles, ensuring secure and authorized access. Indeed, the SCAS interfaces seamlessly with the blockchain network to authenticate and verify the credentials of incoming vehicles. Through this integration, the system cross-references the provided car credentials with the immutable blockchain records to ensure the legitimacy and authorization of each vehicle seeking access. Once authenticated, the system grants or denies access based on the car's authorization level or the availability of parking spaces.

C. CARS AND DRIVERS

Drivers use a mobile application to check slot availability before arriving at their selected parking facility where they initiate the entry process.

D. TRUSTED AUTHORITY

The Trusted Authority (TA) plays a central role in the system's inception, overseeing tasks ranging from driver registration to the issuance of certifications to parking lot owners, thereby granting them the necessary permissions to interact with the blockchain. These tasks are conducted offline prior to the system's activation. In practice, the TA often takes the form of a governmental agency with a vested interest in upholding the security of the parking system as well as relying on parking statistics as a basis for strategic decision-making.

E. BLOCKCHAIN NETWORK

Our proposed scheme centers around a layered Blockchain network, serving as the backbone for decentralized parking services. This blockchain network can serve as a secure, transparent, and efficient platform for managing parking-related data, authentication, and authorization processes. It can enhance trust, reduce fraud, and improve the overall functionality of the parking system. Moreover, transactions on the blockchain are conducted in real-time over the internet.

IV. ARCHITECTURE SPECIFICATIONS

This section provides insight into the main contributions of each module within the overall architecture and how they collaboratively work to deliver an integrated solution. Figure 2 shows the architecture of the PufParkChain system.

A. PARKING RECOMMENDATION SYSTEM

A parking recommendation system is designed to help users find personalized parking spot based on their past experience. The system typically has a user-friendly interface, often in the form of a mobile app, allowing users to easily access and utilize its features. Indeed, the driver consult real-time information from his mobile app about parking space availability in various locations. All the data is collected from sensors to determine which parking spots are vacant and which are occupied.

B. CAR AUTHENTICATION

The car arrives at a parking spot based on the system's recommendation. When a vehicle approaches the parking area, sensors detect its presence, and at the parking entrance, a specialized circuit employs Bluetooth technology in an attempt to read the car's SRAM PUF (Physical Unclonable Function). The SRAM PUF is a hardware-based security feature that leverages the unique characteristics of individual SRAM cells to create a unique and unclonable identifier for the car. This identifier can be used for secure authentication and access control purposes. Using Bluetooth technology, the parking entry circuit communicates with the car's onboard system to request the SRAM PUF data. The car's system responds by providing the SRAM PUF data, which is a cryptographic key or code unique to that specific vehicle. The entry circuit then verifies the received SRAM PUF data against the data of authorized SRAM PUFs which is securely stored within the blockchain. If the SRAM PUF matches an entry in the blockchain and the car is authorized for access, the entry gate automatically opens, allowing the vehicle to enter. Simultaneously, the system logs the entry time and associates it with the vehicle's record then save it into the blockchain network for billing and tracking purposes. In cases where the SRAM PUF data does not match an authorized entry or there is an issue with the Bluetooth communication, the system denies entry and may

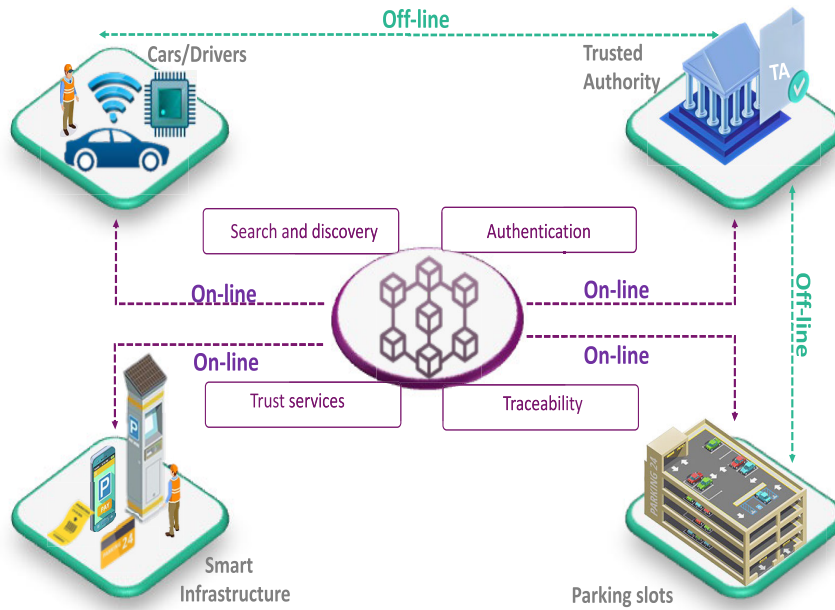


FIGURE 1. Overview of pufparkchain system.

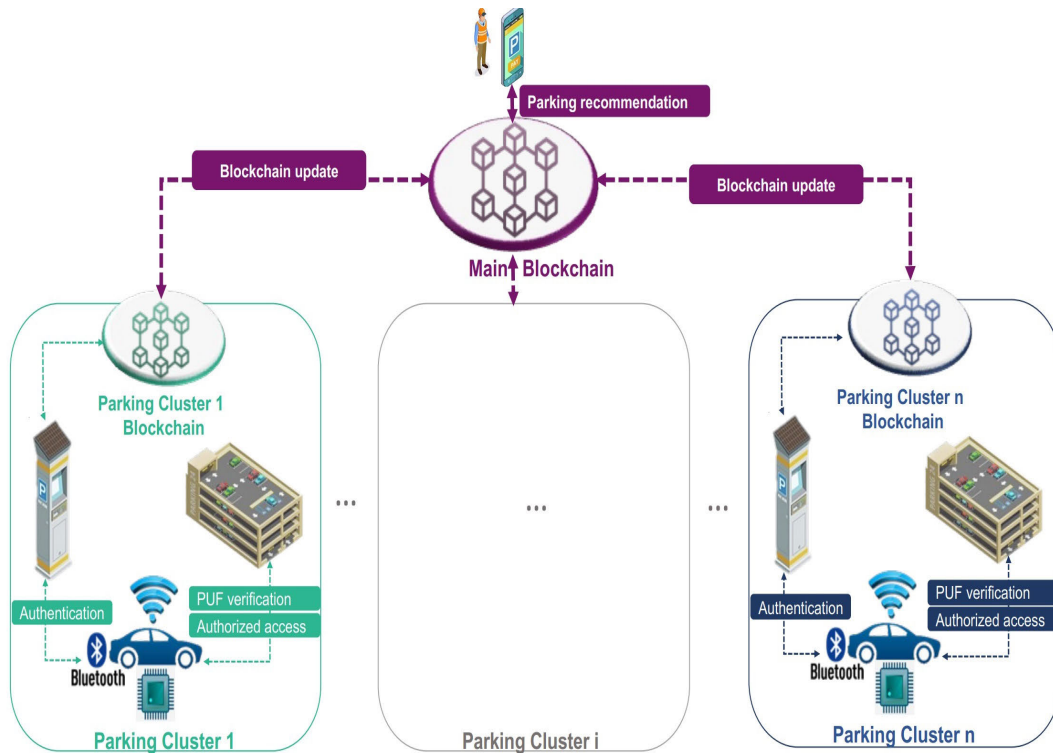


FIGURE 2. PufParkchain architecture.

display a message instructing the driver to contact parking management.

1) SRAM-PUF DESCRIPTION

The specific concept of the SRAM Physical Unclonable Function (PUF) was introduced [17] by Guajardo, Kumar, and Schrijen in 2007. This work presented the idea of using

the inherent variations in SRAM cells on field-programmable gate arrays (FPGAs) to generate unique and unpredictable responses that could be used for purposes like device authentication and IP protection.

Since SRAM circuits are commonly used in many SoCs, we choose to include SRAM PUFs as a security feature for the vehicle authentication in smart parkings. Thus, this solution

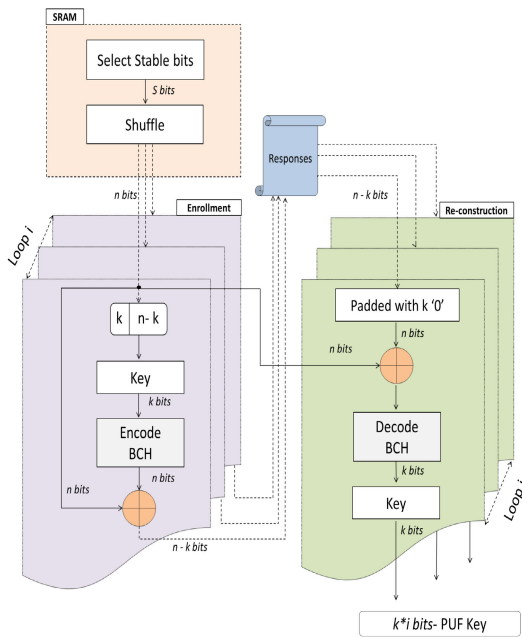


FIGURE 3. Enrollment and PUF generation.

conducts to a low Area Overhead with more space-efficient option compared to other dedicated PUF circuits that require additional resources.

In order to generate the PUF key, two processes are performed:

- **Enrollment:** During this phase, the circuit is subjected to a series of challenges or stimuli, and the corresponding responses are measured and recorded. Once the enrollment phase is completed, the unique stored responses serve as the basis for cryptographic key generation.
- **Reconstruction:** It consists on reconstructing a cryptographic key or generating a response based on the stored responses obtained during the enrollment phase. Indeed, selected challenges are applied to the SRAM PUF circuit and the generated responses are compared to the stored responses previously stored. Based on the comparison of responses, a cryptographic key or a derived response is generated. This can involve mathematical operations, error correction techniques, or statistical models to extract the desired key or response from the measured responses.

Figure 3 describes the steps, algorithms and the tools used to generate the PUF Key from an SRAM circuit.

a: SRAM PROCESSING

During the generation of SRAM PUF, it is important to select stable bits. Indeed, SRAM PUFs rely on the inherent process variations that occur during the manufacturing of SRAM cells. These process variations result in stable and unique electrical characteristics for each SRAM cell.

The selection of stable bits involves identifying the SRAM cells that exhibit consistent behavior and have minimal susceptibility to environmental variations, such as

temperature or supply voltage fluctuations. These stable bits are then used to create the unique challenge-response pairs (CRPs) during the enrollment phase.

Several algorithms are used to select stable bits such as the Temporal Majority Voting algorithm (TMV) [24], Neighborhood-based Bit Selection (NBS) [40], the Data Remanence Analysis (DRA) [25], and Systematic Selection method (SS) [39]. The TMV approach focuses on observing the stability of individual bitcells during the power-up process. By monitoring the consistency of a bitcell's value over a certain number of consecutive observations, stable cells can be identified.

For the NBS, authors observed that a strong stable cell is consistently found in the vicinity of other stable cells. This indicates a correlation or pattern where neighboring cells contribute to the stability of a particular cell. Consequently, authors performed multiple power-up operations to gather a sufficient sample the power-up states of the SRAM cells. Each cell was assigned a weight value (correspondingly to the power-up samples) and a window size (correspondingly to the number of neighbors). The identification of stable cells and select strong stable cells is based on weight values, window size, and threshold criteria of these parameters, with considerations for different environmental conditions.

The DRA method involves analyzing the residual representation of data in SRAM cells after power-off to identify stable bits. It consists only on two remanence tests. This method encompasses writing either '1' or '0' throughout the array and briefly cutting off the power supply until a small number of cells switch states. This strategy exploits the inherent characteristic that the cells which can be effortlessly switched represent the most robust cells when programmed with opposite data. Finally, the SS method aims to control the power supply ramp rate in order to identify the cells in the SRAM that are strongly biased, thereby resistant to circuit noise, voltage and temperature changes.

Strong bit selection in [24], [39], and [40] requires complex and exhaustive experiments and analysis in order to determine the best parameters and thresholds. In addition, the experimental results are sensitive to variations in these environmental factors and the power supply rates, which could affect the reliability and robustness of the selected stable cells.

In this paper, we considered the Data Remanence Analysis since it requires a shorter time to select stable bits compared to the other studied algorithms. In the other side, we conducted several tests in order to accurately ascertain the duration of the temporal power down of the SRAM circuit.

After the studied phase, a number S of stable bits is selected. S should be big enough to generate the SRAM PUF key. In this case, we select randomly the required bits to feed the next enrollment phase.

b: ENROLLMENT PHASE

The enrollment and the re-construction processes are based on the fuzzy extractor proposed by [21]. The previously

selected stable bits are used as challenges to generate the helper data during the enrollment for a cryptographic application. Indeed, several steps are involved. First, the selected stable bits are divided into words of n bits representing the challenge data. These stable bits likely contain crucial information or key material for the cryptographic system. Next, k bits of the key are encoded using the BCH error-correcting code. This encoding process helps in detecting and correcting errors that may occur during data transmission or storage, ensuring the integrity of the information. Once the k bits are encoded with the BCH code, they are further processed by XORing them with the initially selected challenge. This step serves to obfuscate the helper data and make it even more challenging for potential adversaries to decipher or manipulate.

c: RE-CONSTRUCTION PHASE

The re-construction process involves during the authentication step of the vehicle using the helper data generated during the encoding phase to reconstruct the original secret key. The car's permission to enter the parking area is subject to the validation of the generated key. In this crucial phase, the previously generated helper data is retrieved from secure storage. Subsequently, it undergoes an XOR operation with the challenge data, forming an integral part of the process. Following this step, the combined data is meticulously subjected to BCH decoding, a specialized error-correction procedure that plays a pivotal role in unveiling the hidden information.

C. BLOCKCHAIN NETWORK

Blockchain plays a pivotal role in authentication by securely storing and verifying digital identities and transactions. It provides a tamper-resistant, decentralized ledger that ensures the integrity and immutability of authentication data. This technology helps establish trust, eliminates the need for intermediaries, and enhances security by enabling transparent and verifiable authentication processes. Blockchain's role in authentication extends to various applications, including identity verification and access control in the parking systems.

The PuffParkChain system contains a lightweight architecture of the hybrid blockchain network which includes a set of full and light nodes. This architecture is composed mainly by:

- The main blockchain which communicates with the clusters located at the city/department level. This blockchain contains all the data retrieved from all the parkings. The primary advantage of the main blockchain is to keep a record of all transactions conducted in the various parking lots for potential analysis later.
- A local blockchain for each parking cluster where a cluster is composed of one or a few parking lots that are physically close. Each local blockchain is established as an integral component of the overarching blockchain. This local blockchain stores mainly 2 types of data:

- The blocks containing the PUF keys of vehicles registered by the trusted authority.
- The blocks containing the data pertaining to vehicles that have authenticated and accessed this parking.
- the headers of blocks containing transactions from other local blockchains

The main advantage of this local blockchain is to reduce the vehicle authentication time at the parking entrance.

In the proposed system, the main blockchain relies on cloud servers (CS), which act as complete/full blockchain nodes. These servers store a full copy of the blockchain, participate in transaction validation and generate blocks. Indeed, Servers can establish connections with one of several strategically positioned gateways located at designated parking slots. These gateways serve as ingress points, facilitating the transmission of transactions to the servers. Subsequently, these servers collaborate in the critical process of block validation, working in tandem with other server nodes that implement the consensus algorithm to ensure the integrity and agreement of the network's transaction ledger.

On the other hand, a local blockchain of one cluster is formed by a set of lightweight nodes (N) located at the parking level as well as a local gateway (G) to communicate with a corresponding cloud server of the main blockchain. The parking area is strategically designed with multiple entry points, and this deliberate layout not only promotes effective communication between all nodes situated at these entry points and the central gateway but also greatly facilitates the entrance of vehicles into the parking facility. This design ensures a streamlined and efficient process for vehicles accessing the parking area. All the nodes of a given cluster serve as IoT systems, gathering data not just on parking space occupancy and vehicle entrance, but also on cars moving within the parking area. Thus being a lightweight nodes are well-suited for those IoT devices with limited computational and storage resources.

Figure 4 presents the workflow of the blockchain networks of the proposed system. The initial step (1) entails the enrollment of all vehicles under the jurisdiction of a trusted authority to acquire their Physically Unclonable Function (PUF). Following the registration and acquisition of the (PUF), this unique identifier is securely stored within the blockchain network. The block also contains essential information about the car, including details like the owner's name, the fabrication date, the registration plate, and other pertinent data. Through this registration, the vehicle is now granted access to all the parking facilities covered by the blockchain network. If any of the vehicle's parameters change, especially ownership, an update is made in the blockchain with the same unique identifier of the car, which the SRAM PUF derived from its electronic board/ or the registration plate. Therefore, if the car's electronic card is damaged and needs replacement, the owner must report and justify this change to the trusted authority (TA), which will proceed to deactivate the old account and create a new

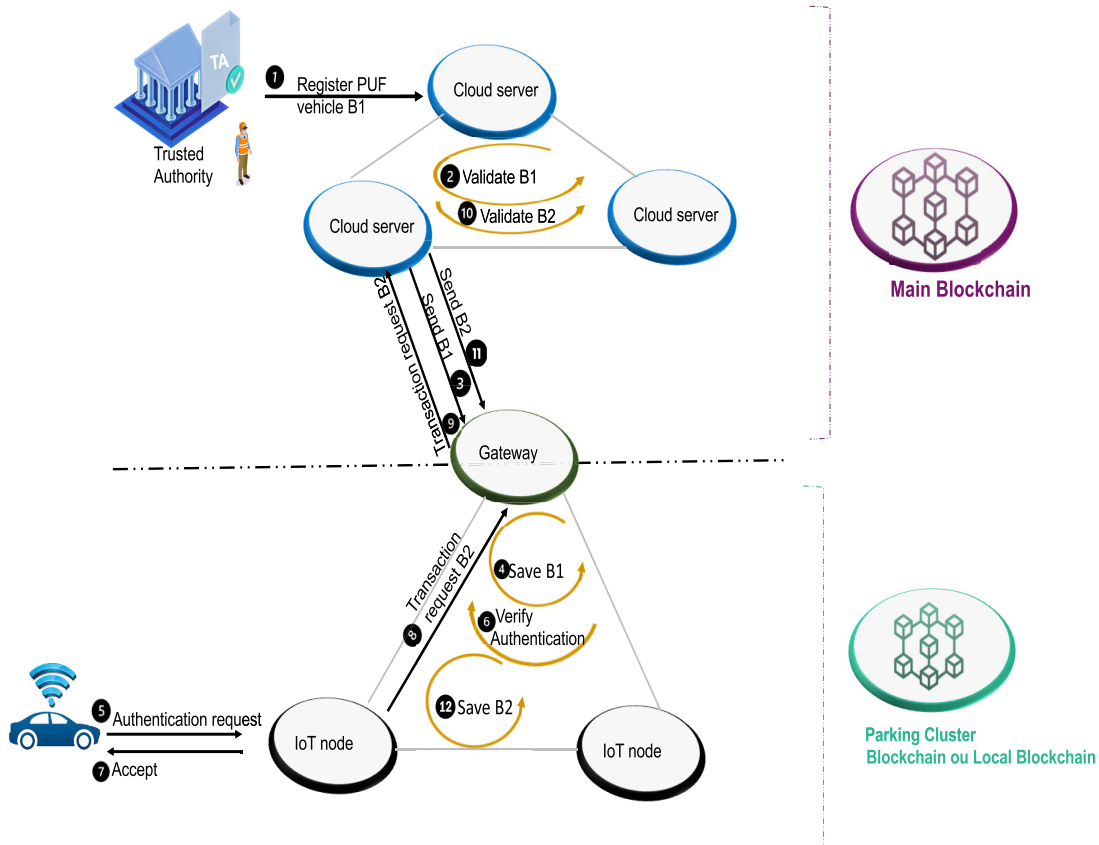


FIGURE 4. Workflow of PufParkChain system.

record with updated parameters. The registration transaction is initially received by a cloud server (CSi) and subsequently validated (2) by the other cloud servers through a consensus protocol, ensuring accuracy and authenticity of the data. Moreover, the (CSi) disseminates the received block from the trusted authority to all other cloud servers which carries out the verification of the block's transactions for legitimacy by scrutinizing the signature of each transactions. Then the (CSi) receives the responses of all cloud servers in order to make a decision about whether to include this block in the blockchain or not. If the block is valid, each cloud server seamlessly integrates the new block into its blockchain and then efficiently transmits it to its clusters through gateways (3). Each cloud server can be connected to one or multiple gateways which have their own parking cluster. This synchronized action ensures that all pertinent nodes within the clusters have access to the most current and consistent blockchain data. Within a parking cluster, every gateway conducts a thorough examination of the incoming block to identify transactions originating from the (TA). When such transactions are detected, the gateway not only retains and stores the full block in its local blockchain but also forwards it to the connected IoT devices to be validated (4).

The IoT devices extract the block header and store it into their blockchain due to their limited hardware resources.

On the other side, when a vehicle arrives at a parking facility and, a Smart Access Control System (SACS) comes into action to respond to the authentication request of the vehicle (5). It employs short-range communication technology, such as Bluetooth, to seamlessly read the unique Physically Unclonable Function (PUF) of the car. Subsequently, the system meticulously checks into the blockchain network to ascertain whether this particular vehicle is granted permission to access the premises, effectively ensuring a seamless and secure entry process (6). The SACS seeks for the vehicle information from the local cluster gateway by sending a specific request which contains the PUF of the vehicle. The gateway, in response, initiates a search within its local blockchain. If the requested block exists and the car is registered, the gateway promptly responds by furnishing the relevant block containing the data and the details of this car. If the block does not exist within the local blockchain, that means that the vehicle is not registered and then, it signifies that it is not authorized to access the parking facility. When the car is authorized, the Smart Access Control System (SACS) grants permission for the vehicle

to enter the parking facility (7). As the car's entrance into the parking is confirmed by the IoT system, it initiates a transaction to the nearest gateway (Gi) in the parking cluster(8), conveying entrance details such as the car's PUF and the timestamp of entry. This transaction record serves to maintain a comprehensive log of the vehicle's access and entry details. The Gateway (Gi) forwards the block to the specific cloud server (CSi) to which it is directly connected (9), and the cloud server then proceeds to broadcast this block (10) to other servers for validation, following the procedure detailed in the step (2). After the block is validated and integrated into the blockchain of each cloud server, it is disseminated to all gateways (11). Each gateway performs a check to confirm if the transaction originated within its specific cluster. If it does, the gateway retains the entire block and distributes it to other IoT nodes (12), following the process explained in step (4). If the transaction is originated from other cluster, the gateway validates the block, retains only the block header while discarding the block data and then sends it to the IoT devices of the same cluster. These IoT nodes perform the same steps as the gateway. This selective storage approach ensures efficient data management and distribution.

As a result, each cluster maintains complete records of all the transaction blocks originating from the parking facility. This local storage ensures comprehensive traceability of all vehicles entering the parking area, which enables not only a local processing tasks such as calculating individual car fees with precision and efficiency but also significantly reduces processing time.

On the other side

V. PERFORMANCE EVALUATION

In this section, we will describe the implementation of the PUF function and demonstrate its functionality through a concise scenario as follows: When a sensor detects the presence of a vehicle, the SCAS analyzes the Bluetooth devices that have been newly connected. The SCAS then sends an "OK" message to the newly connected vehicle. Upon receiving the "OK" signal, the vehicle calculates the Physical Unclonable Function (PUF) key as described in the paper. The vehicle sends the calculated PUF key in string form back to the SCAS which verifies the received PUF key against the blockchain-stored one. The authentication decision can be displayed on an LCD screen or on the access barrier, allowing or denying access to the parking facility. Finally, we assess its performance, and subsequently conduct a comprehensive security analysis of the proposed system.

A. SRAM EVALUATION

In our PUF implementation, we opted for the Cypress CY62256NLL, a readily available 256Kb SRAM known for its superior stability compared to other off-the-shelf SRAMs [30]. To select the most suitable candidate for PUF generation, we conducted evaluations on three SRAM circuits, designated as C1, C2, and C3. The evaluation process

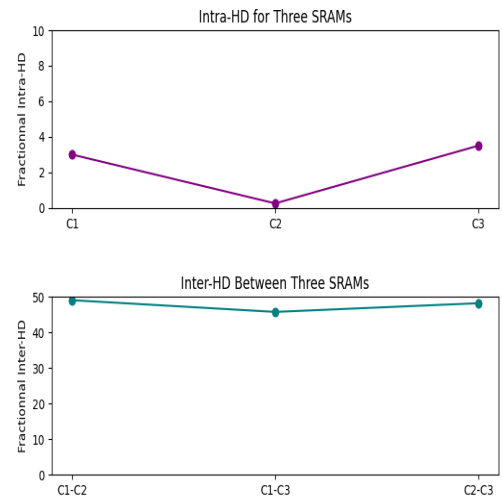


FIGURE 5. Intra-HD and Inter-HD for Tested SRAMs.

involved assessing the Hamming distance, which quantifies the dissimilarity between two sequences of equal length (in our context, the bit sequences read from the SRAMs). This distance metric is calculated as the number of positions at which the corresponding bits differ.

Our evaluation focused on both inter-circuit and intra-circuit Hamming distance (HD). Inter-circuit HD measures the dissimilarity between the bit sequences of the same address in different SRAM circuits (C1, C2, and C3), providing insights into the variability between these circuits. Conversely, intra-circuit HD evaluates the stability of each SRAM circuit by comparing the bit sequences read from the same address at different times or under different conditions.

Specifically, we utilized fractional representations to quantify the intra-circuit and inter-circuit Hamming distance (HD) in our evaluation. These fractional representations are derived from the following equations:

$$\text{Intra-HD} = \frac{\text{Nbr of diff bits within the SRAM}}{\text{Total number of bits compared}} \times 100\% \quad (1)$$

$$\text{Inter-HD} = \frac{\text{Nbr of diff bits between SRAMs}}{\text{Total number of bits compared}} \times 100\% \quad (2)$$

For an ideal SRAM, the intra-HD, representing the variability within the same SRAM circuit, should ideally be 0%, indicating perfect stability and consistency in the stored bit values. On the other hand, the inter-HD, reflecting the variability between different SRAM circuits, should ideally be 50%, suggesting that each SRAM circuit is unique and produces distinct responses, a desirable characteristic for PUF applications to ensure uniqueness and unpredictability.

Figure 5 displays the results of the intra-HD and inter-HD measurements conducted at room temperature. These results were obtained using a total of 2331 bits for analysis and 8 measurements on each SRAM.

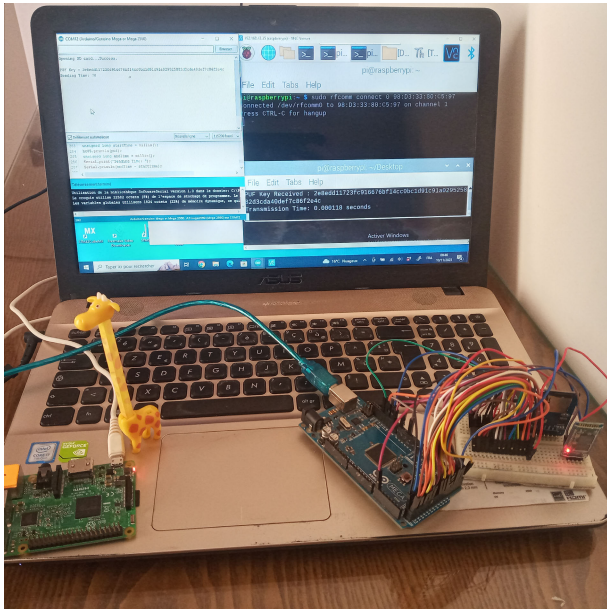


FIGURE 6. Implementation environment.

The results indicate that the average inter-circuit Hamming distance (inter-HD) among the three tested circuits is 47.67%, which is deemed acceptable. Conversely, the average intra-circuit Hamming distance (intra-HD) is found to be 2.25%. These values provide insight into the stability and uniqueness of the circuits, with lower intra-HD values indicating greater stability within individual circuits and a higher inter-HD suggesting distinctiveness between different circuits.

B. PUF EVALUATION

In our pursuit to validate the PUF mechanism, we executed the SRAM PUF implementation by interfacing an Arduino Mega board with a Cypress CY62256NLL. The Mega offers 54 digital GPIO pins, which is significantly more than other Arduino boards, making it suitable for PUF implementation that require a large number of connections especially to interface with the SRAM circuits efficiently, ensuring reliable communication and data exchange. The Arduino Mega orchestrates the enrollment phase, during which essential helper data is meticulously generated and securely stored on an SD card reader.

For the authentication process, a Raspberry Pi 3 board was employed to extract the SRAM PUF data from the off-the-shelf SRAM module, establishing a seamless Bluetooth communication link between the Raspberry Pi and the Arduino Mega, employing the HC-05 Bluetooth module.

Notably, the Raspberry Pi board also operates as a lightweight node on the local blockchain, further contributing to the system's integrity. Leveraging this capability, it can facilitate the transmission of authentication requests to the nearest gateway within the blockchain network. Figure 6 illustrates the complete environment.

Furthermore, in reference to figure 3, we have established the parameters for the fuzzy extractor function by considering the resources constraints of the selected hardware board. First of all,

Due to the hardware constraint of the Arduino Mega, which has a limited SRAM size of 8KB, we have selected the parameters $k=7$ bits and $n=63$ bits for the implementation of the BCH code as described in [9]. The selected parameters require 4335 KB of SRAM memory, a requirement that is met by the Arduino Mega platform. These parameters signify that each code word consists of 63 bits in total, with 7 of those bits carrying the actual information (message bits), and the remaining bits serving as redundancy. This configuration allows for efficient error detection and correction while staying within the memory limitations of the Arduino's SRAM. Consequently, the complete PUF key generation is performed using a number of i iterations determined by the following equation:

$$i = l/k \quad (3)$$

With l is the length of the PUF key and k is the number of information bits in the codeword. Thus 37 loop iterations are required to generate a 256-PUF key. Finally, the number of stable bits S is determined by the following equation:

$$S = i * n \quad (4)$$

In our implementation S equates 2331 stable bits.

We completed the implementation of the Physical Unclonable Function (PUF) on the Arduino board with the selected parameters. Notably, during the implementation process, we meticulously measured the execution time of the main functions, ensuring that the PUF operates efficiently and meets the demanding requirements of our specific use case which is the vehicle authentication. Figure 7 shows the execution time of the main functions from the PUF implementation. We conducted the experiment three times for each function, and for each iteration, we recorded the execution time. The reported values for the execution times are the averages obtained from these three repetitions, providing a more reliable representation of the typical performance of each function. These results are explained as follows:

- The *Read SRAM* function indicates the time taken to read data from the Static Random-Access Memory (SRAM). It's a relatively high execution time which is primarily attributed to its dual-step composition. Firstly, there is an imperative need to access the SD card in order to retrieve the indices corresponding to the stable bits. This process inherently associated with increased time overhead due to the comparatively slower access speeds of SD cards (10Mb/s). Then, the subsequent step involves accessing the Static Random-Access Memory (SRAM) component to read the states of the identified stable bits. The SRAM access is integral to obtaining the specific data points required for subsequent operations.

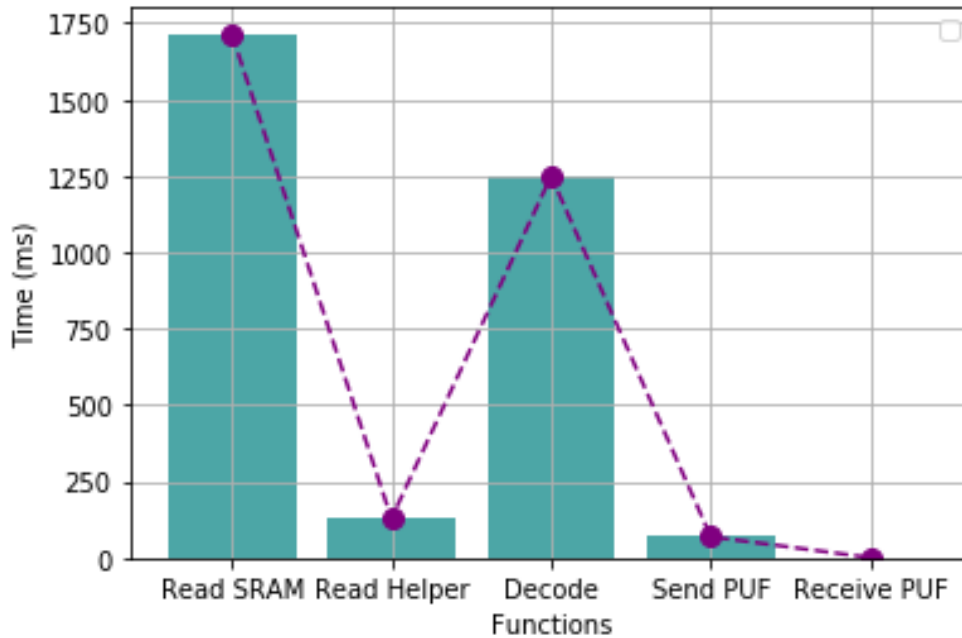


FIGURE 7. Execution time of PUF functions.

- The *Read helper data* function from SD card shows the time taken to read the response data from the SD card. This data is stored into the SD card during the enrollment phase.
- The *Decode* function indicates the time taken to perform the BCH decode algorithm as well as XORing the SRAM data with the helper data.
- The *Send PUF* function represents the time taken to send the PUF data from an Arduino Mega through HC-06 Bluetooth module using a baudrate of 9600 b/s.
- The *receive PUF* function indicates the time taken to receive the PUF data on the Raspberry Pi through bluetooth communication.

The overall execution time (3162.125ms) is deemed acceptable, considering the constraints of the Arduino Mega board, which operates with a limited frequency (16MHz). Many of the functions were executed on this board, and the observed times reflect the performance achievable within these constraints. It's worth noting that transitioning to a more sophisticated processor with higher processing capabilities could further enhance the overall efficiency of the PUF generation process.

C. SECURITY ANALYSIS

The proposed PufParkChain system has been meticulously designed to fortify itself against potential security issues.

The following attack scenarios are outlined:

- An attacker might steal the hardware security module (the PUF device) and can clone the device. Nevertheless, even having a PUF device in hand, direct generate the PUF key is still impossible without knowing the

selected stable bits which are externally stored. Indeed, in this paper, the size of the used SRAM is equal to 262144 bits (256Kb), thus the number of the possibilities to get 2331 stable bits is calculated from the permutation formula 5.

$$P(65536, 2331) = \frac{262144!}{(262144 - 2331)!} \quad (5)$$

The sheer magnitude of potential arrangements, represented by an enormous number of possibilities, renders any attempt to divine or predict the specific stable bits randomly shuffled and selected during the enrollment phase, practically infeasible. The complexity and scale of the permutation space create a formidable challenge for unauthorized access or manipulation.

- An attacker steal the SD card (or any external storage) in which the indices of the stable bits are stored as well as the helper data. Even in the event of an SD card theft, unauthorized access to the PUF key remains unattainable. This is due to the fact that obtaining the key requires accessing the SRAM memory to read the states of the stable bits. The number of possibilities of the SRAM challenges is equal to 2^{2331} since each bit can be 0 or 1. It is considered as an extremely large number, reflecting the vast number of possible combinations.
- Given the short-range nature of Bluetooth communication and the carefully designed parking infrastructure, the proximity required for authentication makes it challenging for any unauthorized entity or vehicle to approach the target vehicle during the authentication process. This spatial constraint serves as a deterrent,

mitigating security threats such as Man-in-the-Middle attacks.

Hence, we are confident in the security of our proposed data and The PUF key-based vehicle authentication. The sole viable method for an attacker to access the PUF key is by possessing both the PUF device and the external storage card.

D. SCALABILITY ANALYSIS

Scalability is a critical factor in the design and implementation of modern parking management systems. As urban populations grow and the demand for parking increases, it is essential for parking solutions to be able to scale efficiently to meet these demands. In this section, we discuss the scalability of our parking management solution, focusing on how it addresses key challenges related to system expansion, resource allocation, and performance optimization. Our solution addresses scalability at multiple levels, including infrastructure scalability and operational scalability.

- At the infrastructure level, our system is designed to easily integrate with existing parking infrastructure and scale up to accommodate additional parking spaces and sensors. Indeed, our solution focuses on integrating key components such as sensors, gateways, and access control modules into existing parking infrastructure. This ensures that the proposed solution can adapt to the changing needs of urban environments without requiring significant modifications to the underlying infrastructure.
- Operational scalability is another key aspect that our solution addresses by proposing a set of clusters connected to the cloud. These clusters distribute parking management tasks efficiently, reducing the workload on individual devices and improving system performance. This approach allows our solution to scale seamlessly as the number of parking spaces and sensors increases, ensuring that it can meet the demands of urban environments without compromising performance or reliability. Additionally, our solution's modular design enables easy integration of new clusters as needed. Some transactions could be managed within the same cluster, while others will be processed at the cloud level, depending on the specific requirements of the parking management system. This hybrid approach optimizes resource allocation and task scheduling, further enhancing the operational scalability of our solution. Moreover, our solution could be used to build a hierarchical clustered architecture for parking management. This architecture would organize parking spaces, sensors, gateways and cloud nodes into clusters based on their geographic locations and operational requirements. By clustering these elements, we can optimize the management of parking resources and reduce the overall complexity of the system. Using hierarchical clustering allows us to improve the efficiency of our parking management system in several ways. First, it enables us to reduce the delay overhead associated with processing a large number of parking

requests. By distributing the workload among cluster heads, we can parallelize tasks such as parking space allocation and payment processing, leading to faster response times for users. Additionally, the hierarchical clustering framework allows to dynamically adapting to changing conditions in the parking environment. For example, if certain areas experience high demand for parking spaces, the framework can redistribute resources to accommodate the increased demand. This flexibility ensures that our parking management system remains responsive and efficient under varying conditions. Overall, the use of hierarchical clustering in our parking management system enhances scalability, improves resource utilization, and ultimately provides a better parking experience for users.

VI. CONCLUSION AND FUTURE WORK

In this paper, we presented our PufParkChain solution that integrates a lightweight blockchain network enhancing the overall user experience and operational effectiveness. This network is strategically designed to ensure efficient latency in car authentication while optimizing storage resource requirements for IoT nodes. Car authentication is executed with a strong emphasis on security, leveraging the Physically Unclonable Function (PUF) for enhanced protection and reliability.

Furthermore, we have provided a comprehensive exposition of the PUF mechanism's implementation, coupled with an in-depth security analysis of the proposed system. This dual focus on implementation and security assessment ensures a thorough and well-rounded understanding of our solution's robustness and functionality. The Overall execution time of the PUF key is estimated to 3s using an arduino mega platform.

In addition to the technical implementation, our authentication system using Physical Unclonable Functions (PUF) has significant implications for the development of smart city solutions, particularly in the realm of parking management. By leveraging PUF for authentication, our system enhances the security and reliability of smart parking systems, ensuring that only authorized vehicles can access parking facilities. This not only reduces the risk of unauthorized access but also contributes to the efficient use of parking spaces, thereby reducing congestion and improving the overall flow of traffic in smart cities. Furthermore, the data collected from our authentication system can be used to optimize parking management strategies, such as pricing policies and parking space allocation, leading to more effective and sustainable use of urban parking resources. These benefits highlight the potential of our authentication system to not only improve the security of parking facilities but also to enhance the overall efficiency and sustainability of smart city infrastructure. For the future works, we aim to improve the proposed PufParkChain with the following features:

- Develop a tailored consensus mechanism specifically designed for the smart parking system. This custom

consensus protocol will be meticulously crafted to address the unique demands and requirements of the smart parking environment, optimizing security, scalability, and efficiency for the benefit of both users and administrators.

- We intend to securely archive the responses and relevant helper data associated with each vehicle within an IPFS (InterPlanetary File System) repository. This approach is designed to mitigate the reliance on local storage within the vehicle, thereby enhancing data security.
- We aim to leverage a more sophisticated hardware platform for PUF key generation to enhance the efficiency of the vehicle authentication process. By upgrading to an advanced board, we anticipate a significant acceleration in the authentication workflow, ensuring faster and more seamless verification of vehicles within our system.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interests regarding the publication of this paper.

REFERENCES

- [1] S. Das and R. Kayalvihzi, "Advanced multi location IoT enabled smart car parking system with intelligent face recognition," *Int. J. Res. Eng., Sci. Manag.*, vol. 7, no. 1, pp. 1–6, 2024.
- [2] H. Y. P. Napitupulu and I. G. D. Nugraha, "Fog computing-based system for decentralized smart parking system by using firebase," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 13, no. 1, pp. 44–52, 2024.
- [3] A. Fahim, M. Hasan, and M. A. Chowdhury, "Smart parking systems: Comprehensive review based on various aspects," *Heliyon*, vol. 7, no. 5, May 2021, Art. no. e07050.
- [4] A. Aditya, S. Anwarul, R. Tanwar, and S. K. V. Koneru, "An IoT assisted intelligent parking system (IPS) for smart cities," *Procedia Comput. Sci.*, vol. 218, pp. 1045–1054, 2023.
- [5] S. Rajbhandari, B. Thareja, V. Deep, and D. Mehrotra, "IoT based smart parking system," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol. (3ICT)*, Nov. 2018, pp. 1–5.
- [6] S. Ahmed, Soaibuzzaman, M. S. Rahman, and M. S. Rahaman, "A blockchain-based architecture for integrated smart parking systems," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2019, pp. 177–182.
- [7] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (PUF) for IoT devices," *ACM Comput. Surveys*, vol. 55, no. 14s, pp. 1–31, Jul. 2023.
- [8] A. H. Alavi, P. Jiao, W. G. Buttler, and N. Lajnef, "Internet of Things-enabled smart cities: State-of-the-art and future trends," *Measurement*, vol. 129, pp. 589–606, Dec. 2018.
- [9] BCH. (1994). *Error Codes Page*. Accessed: Nov. 13, 2023. [Online]. Available: <https://www.eccpage.com/>
- [10] C. Biyik, Z. Allam, G. Pieri, D. Moroni, M. O'Fraifer, E. O'Connell, S. Olariu, and M. Khalid, "Smart parking systems: Reviewing the literature, architecture and ways forward," *Smart Cities*, vol. 4, no. 2, pp. 623–642, Apr. 2021.
- [11] O. Cheikhrouhou, K. Mershad, F. Jamil, R. Mahmud, A. Koubaa, and S. R. Moosavi, "A lightweight blockchain and fog-enabled secure remote patient monitoring system," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100691.
- [12] C. Cheisviyanny, A. Rasli, S. Dwita, Deviani, and V. F. Sari, "Illegal parking attendants and parking (mis)management: A case study in Padang, west Sumatra, Indonesia," *Asian Transp. Stud.*, vol. 9, 2023, Art. no. 100118.
- [13] L. N. CheSuh, R. Á. Fernández-Díaz, J. M. Alija-Perez, C. Benavides-Cuellar, and H. Alaiz-Moreton, "Improve quality of service for the Internet of Things using blockchain & machine learning algorithms," *Internet Things*, vol. 26, Jul. 2024, Art. no. 101123.
- [14] M. T. D. Oliveira, L. H. A. Reis, D. S. V. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. F. Mattos, "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," *Comput. Netw.*, vol. 179, Oct. 2020, Art. no. 107367.
- [15] A. O. Elfaki, W. Messoudi, A. Bushnag, S. Abuzneid, and T. Alhmedat, "A smart real-time parking control and monitoring system," *Sensors*, vol. 23, no. 24, p. 9741, Dec. 2023.
- [16] A. Floris, S. Porcu, L. Atzori, and R. Girau, "A social IoT-based platform for the deployment of a smart parking solution," *Comput. Netw.*, vol. 205, Mar. 2022, Art. no. 108756.
- [17] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptograph. Hardw. Embedded Syst.*, 2007, pp. 63–80.
- [18] H. S. Jennath, S. Adarsh, N. V. Chandran, R. Ananthan, A. Sabir, and S. Asharaf, "Parkchain: A blockchain powered parking solution for smart cities," *Frontiers Blockchain*, vol. 2, Aug. 2019.
- [19] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," *Sci. Rep.*, vol. 14, no. 1, Apr. 2024.
- [20] W. A. Jabbar, C. W. Wei, N. A. A. M. Azmi, and N. A. Haironnazli, "An IoT raspberry pi-based parking management system for smart campus," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100387.
- [21] H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura, "Cryptographic key generation from PUF data using efficient fuzzy extractors," in *Proc. 16th Int. Conf. Adv. Commun. Technol.*, Feb. 2014, pp. 23–26.
- [22] A. Khariche, S. Badholia, and R. K. Upadhyay, "Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India," *Blockchain, Res. Appl.*, Jan. 2024, Art. no. 100188.
- [23] M. Kim and Y. Kim, "Multi-blockchain structure for a crowdsensing-based smart parking system," *Future Internet*, vol. 12, no. 5, p. 90, May 2020.
- [24] L. Lam, "Theory and application of majority vote: From condorcet jury theorem to pattern recognition," in *Proc. 2nd Int. Conf. Math. Educ. 21st Century, Math. Living*, Nov. 2000.
- [25] M. Liu, C. Zhou, Q. Tang, K. K. Parhi, and C. H. Kim, "A data remanence based approach to generate 100% stable keys from an SRAM physical unclonable function," in *Proc. IEEE/ACM Int. Symp. Low Power Electron. Design (ISLPED)*, Jul. 2017, pp. 1–6.
- [26] Y. Liu, *Mobile Crowdsensing: Issues and Challenges*. Cham, Switzerland: Springer, 2020, pp. 861–865.
- [27] R. Looknuang, K. Nambut, and S. Usanavasin, "Smart parking using IoT technology," in *Proc. 5th Int. Conf. Bus. Ind. Res. (ICBIR)*, May 2018, pp. 1–6.
- [28] S. Mudaliar, S. Agali, S. Mudhol, and C. Jambotkar, "IoT based smart car parking system," *Tech. Rep.*, Jan. 2019.
- [29] A. Sant, L. Garg, P. Xuereb, and C. Chakraborty, "A novel green IoT-based pay-as-you-go smart parking system," *Comput., Mater. Continua*, vol. 67, no. 3, pp. 3523–3544, 2021.
- [30] A. S. Sajim, "Open-source software-based SRAM-PUF for secure data and key storage using off-the-shelf SRAM," Master thesis, 2018.
- [31] M. Solouki and S. M. H. Bamakan, "An in-depth insight at digital ownership through dynamic NFTs," *Procedia Comput. Sci.*, vol. 214, pp. 875–882, 2022.
- [32] S. Tiruvayipati, R. Yellasiri, V. Narayandas, A. Maruthavanan, and A. Meduri, "Methodology for developing an IoT-based parking space counter system using XNO," *Scalable Computing: Pract. Exper.*, vol. 25, no. 2, pp. 800–811, Feb. 2024.
- [33] R. W. Tripuro, A. Giawa, S. Suharyanto, and J. H. Wijaya, "Government policy in illegal parking charges at public spaces," *J. Governance Public Policy*, vol. 10, no. 2, pp. 191–202, Jun. 2023.
- [34] UN. (2018). *UN Department of Economic and Social Affairs, Population Division*. Accessed: Oct. 10, 2023. [Online]. Available: <https://population.un.org/wup/Publications/Files/WUP2018-Highlights.pdf>
- [35] UN Environment Programme (UNEP). (2012). *Global Environmental Outlook 5: Environment for the Future We Want*. Accessed: Oct. 5, 2023. [Online]. Available: <https://sustainabledevelopment.un.org/index.php?page=view&type=400&nr=546&menu=35>
- [36] K. Vijaya, V. G. Krishnan, D. Kumar, B. Laxmi, and B. Yasaswi, "AOA based masked region-CNN model for detection of parking space in IoT environment," *Int. Res. J. Multidisciplinary Technovation*, pp. 97–108, Jan. 2024.

- [37] J. Wang, C. Zhu, C. Miao, R. Zhu, X. Zhang, Y. Tang, H. Huang, and C. Gao, "BPR: Blockchain-enabled efficient and secure parking reservation framework with block size dynamic adjustment method," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3555–3570, Mar. 2023.
- [38] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet Things*, vol. 10, Jun. 2020, Art. no. 100081.
- [39] W. Wang, A. D. Singh, and U. Guin, "A systematic bit selection method for robust SRAM PUFs," *J. Electron. Test.*, vol. 38, no. 3, pp. 235–246, Jun. 2022.
- [40] K. Xiao, Md. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit selection algorithm suitable for high-volume production of SRAM-PUF," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust (HOST)*, May 2014, pp. 101–106.
- [41] H. Zulfiqar, H. M. Ul Haque, F. Tariq, and R. M. Khan, "A survey on smart parking systems in urban cities," *Concurrency Computation: Pract. Exper.*, vol. 35, no. 15, Jul. 2023.



BOUTHAINA DAMMAK was born in Sfax, Tunisia, in 1985. She received the engineering and M.S. degrees from the National Engineering School of Sfax (ENIS), in 2009, and the joint Ph.D. degree in computer science from ENIS, Tunisia, and the University of Valenciennes and Hainaut Cambresis, France, in December 2016. She is currently an Assistant Professor with the Department of Computer Science, Applied College, Princess Nourah Bint Abdulrahman University. Her research interests include multiprocessor architecture, embedded system, and the IoT applications.



MARIEM TURKI received the joint Ph.D. degree in computer science systems from the National School of Engineers of Sfax, Tunisia, and the University of Pierre and Marie Curie–Paris. She is currently an Associate Professor of embedded systems with the Higher Institute of Computer Sciences and Multimedia of Gabes. Her research interests include embedded systems and blockchain applications. She is actively serving as a technical program committee member and a reviewer for many international conferences and journals.

AMNAH ALSHAHRANI received the bachelor's degree in education (computer science), the master's degree in computer science from La Trobe University, Australia, and the Ph.D. degree in computer and information sciences from Strathclyde University, U.K. She is currently an Assistant Professor with the Department of Computer Science, Applied College, Princess Nourah Bint Abdulrahman University.

• • •