HAI, T., AKSOY, M., IWENDI, C., IBEKE, E. and MOHAN, S. 2024. CIA security for internet of vehicles and blockchain-AI integration. *Journal of grid computing* [online], 22(2), article number 43. Available from: https://doi.org/10.1007/s10723-024-09757-3

CIA security for internet of vehicles and blockchain-AI integration.

HAI, T., AKSOY, M., IWENDI, C., IBEKE, E. and MOHAN, S.

2024

This version of the article has been accepted for publication, after peer review (when applicable) and is subject to Springer Nature's AM terms of use, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: https://doi.org/10.1007/s10723-024-09757-3

OpenAIR @RGU

This document was downloaded from https://openair.rgu.ac.uk

SEE TERMS OF USE IN BOX ABOVE

DISTRIBUTED UNDER LICENCE

CIA Security for Internet of Vehicles and Blockchain-AI Integration

Tao Hai

School of Computer and Information, Qiannan Normal University for Nationalities, Duyun, Guizhou, 558000, China
Key Laboratory of Complex Systems and Intelligent Optimization of Guizhou, Duyun, Guizhou, 558000, China
Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA, 40450 haitao@bjwlxy.edu.cn

Muammer Aksoy

Intelligent Medical Systems Department, College of Health and Medical Techniques, Al-Mustaqbal University, 51001, Babylon, Iraq.
Computer Information Systems Department, Ahmed Bin Mohammed Military College, Doha P.O. Box 22988, Qatar; muamer@uomus.edu.iq

Celestine Iwendi

School of Creative Technologies, University of Bolton, A676 Deane Rd., Bolton BL3 5AB, UK
Department of Mathematics and Computer Science, Coal City University Enugu, Enugu 400231, Nigeria; celestine.iwendi@ieee.org

Ebuka Ibeke

School of Creative and Cultural Business, Robert Gordon University, Aberdeen, AB10 7AQ, UK; e.ibeke@rgu.ac.uk

Senthilkumar Mohan

School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, India; senthilkumar.mohan@vit.ac.in

---

Abstract

The lack of data security and the hazardous nature of the Internet of Vehicles (IoV), in the absence of networking settings, have prevented the openness and self-organization of the vehicle networks of IoV cars. The lapses originating in the areas of Confidentiality, Integrity, and Authenticity (CIA) have also

increased the possibility of malicious attacks. To overcome these challenges, this paper proposes an updated Games-based CIA security mechanism to secure IoVs using Blockchain and Artificial Intelligence (AI) technology. The proposed framework consists of a trustworthy authorization solution with three layers, including the authentication of vehicles using Physical Unclonable Functions (PUFs), a flexible Proof-of-Work (dPOW) consensus framework, and AI-enhanced duel gaming. The credibility of the framework is validated by different security analyses, showcasing its superiority over existing systems in terms of security, functionality, computation, and transaction overhead. Additionally, the proposed solution effectively handles challenges like side channel and physical cloning attacks, which many existing frameworks fail to address. The implementation of this mechanism involves the use of a reduced encumbered blockchain, coupled with AI-based authentication through duel gaming, showcasing its efficiency and physical-level support, a feature not present in most existing blockchain-based IoV verification frameworks.

Keywords: Blockchain, Security, Internet of Vehicles, CIA Security, Confidentiality, AI-Game Theory, Authentication, Integrity, Physical Unclonable Functions

1. Introduction

The Internet of Vehicles, commonly referred to as IoV, a branch of the Internet of Things (IoT), is attracting a lot of attention in research and business as the concept of smart cities grows [1]. The IoV has massive potential to reduce energy consumption, the possibilities of traffic accidents, and increase transportation efficiency [2, 3]. In IoVs, the four classifications of Vehicle to Everything (V2X) communication are used in collaboration with flexible mobile networks for the creation of various connections across different networks [4]. Smart transportation systems have the potential to be developed within the framework of V2X connectivity [5]. 'VANETs,' as they are popularly referred to, are evolving into and becoming of greater use to the IoV. While VANETs consist simply of ad-hoc links between vehicles that share data, IoV consists of a bigger network that is inclusive of objects, persons, as well as other heterogeneous networks. Various mobile networks like the fifth generation (5G) technology and long-term evolution are embedded into IoV to create a communication network more stable and extensive than VANETs

currently provide. Transactions and communications between the backbone network and IoV are carried out using ad-hoc networks. IoV makes it possible to collect and share data in the environment, such as the conditions of the road and cars [6].

Some challenges exist regarding the security measures in place in the IoV, which could impact consumers' activities. Security is jeopardized in the event of an intrusion ambush. If attackers can access automobiles, it could lead to traffic accidents. Past experiences have shown how fatal security risks for smart connected vehicles can be when they occur. Fast transmission of information in IoV's security services is common. A sender's right to privacy could be violated if their personal information is divulged from a transmitted communication without protection or encryption. All IoV devices must comply with the three core security standards stipulated below:

- **Confidentiality:** Maintaining the sender's privacy is of utmost importance. This means that any personal information that could identify the sender must be excluded. The content must not contain any hints about the sender's identity; it must be protected by the IoV system.

- **Integrity:** The recipient must receive the data in the exact form in which the sender sent it. To ensure that the data was not tampered with during transit, the system must be capable of detecting any attempts to tamper with it.

- **Authenticity:** A communication could originate from an authorized source or a malicious one. To strengthen the IoV system's security, it must first determine if the node is legitimate. The system must be able to distinguish between legitimate and malicious nodes and handle the malicious nodes accordingly.

Furthermore, the IoV system must strike a balance between emphasizing security and avoiding excessive overhead that might cause delays in broadcasting. Monitoring the vehicles within a network requires them to interact with each other using their unique identifiers. In certain situations, these inter-network communications may include sensitive information. Attackers find it easier to interfere with or intercept network traffic when sensitive information is publicly available. As a result, driver and passenger confidentiality could be seriously compromised.

However, there is an alternative approach that depends on treating each vehicle's identification as a unique stamp to address this challenge. A private key is generated for each vehicle using its unique ID through a private key generator. This approach raises a significant trust challenge, especially in scenarios involving a large number of vehicles. None of the existing options are viable within such constraints. The number of certificates issued and revoked grows with the increasing number of cars on the road, making it vital to detect and identify intruders who disrupt the pattern. This realization has led scholars to recognize the need for more advanced privacy management techniques that can simultaneously trace the identity of the attacker [7].

In the IoV, the services of trusted authorities rely on the vehicle's upload of important data. Conversely, the choices made by the vehicle depend on the services provided by these trusted authorities. This close interaction between vehicles and Roadside Units (RSUs) over wireless channels significantly increases the risk of modified or leaked information. For example, if trusted authorities use inaccurate information to deliver services to automobiles, it could result in financial losses and jeopardize vehicle safety. Therefore, the solution to these challenges involves creating a secure and dependable IoV authentication mechanism [8].

The motivation behind this paper is centered on addressing the cross-trusted authority's CIA (Confidentiality, Integrity, and Authenticity) issues within the IoV using Blockchain technology. The goal is to ensure the safety of information stored on the ledger, decentralize authentication, and use redistributed computation to alleviate the bottlenecks in both trusted authorities and vehicles. The contributions of this paper are listed below:

- To enhance authentication, improve efficiency, and reduce communication time, we introduced Blockchain-enabled RSUs. This innovation shifts a significant portion of the authentication burden to the RSUs.
- Our approach incorporates lightweight cryptographic techniques such as XOR and hash operations, as well as pseudo-random numbers, to decrease the overall computation time of the authentication mechanism.
- The network model of the multi-trusted authorities in our mechanism is more practical. With the use of Blockchain technology, all trusted authorities can utilize a shared ledger for recording vehicle information. This facilitates cross-trusted authentication among authorities and enhances overall effectiveness.

- Our proposed mechanism suggests that vehicles in the first layer should be equipped with Physical Unclonable Functions (PUFs) to provide lower-level authentication using a challenge-response pair gaming method. Additionally, it proposes authentication at the second and third layers using a dual-game technique, thereby ensuring end-to-end authentication [9].

The remainder of this paper is organized as follows: Section 2 provides a background study of IoVs and VANETs, Section 3 proposes the structure for IoV authentication, Section 4 investigates security with a brief formal analysis of potential attack scenarios, Section 5 defends the implementation of our mechanism, offering a comparative analysis with existing studies, and, finally, in Section 6, we conclude the study.

2. Literature Review

In reference to [10], the authors conducted a survey of the Intelligent Transportation System (ITS) and addressed privacy and security concerns affecting VANETs and Vehicular Cloud Computing (VCC). They provided an overview of these concepts and compared trust and cryptography models in relation to different types of attacks. In [11], the authors tackled the issue of users struggling with multiple IDs and passwords for various network services by proposing a flexible ID-based authentication mechanism within a multi-server framework. Experimental results demonstrated its efficiency, offering mutual anonymity and user authentication. Authors in [12] suggested a decentralized, Blockchain-based remote data auditing framework for network storage services. This framework utilized smart contracts to notarize the integrity of outsourced data and employed the Blockchain network for self-recording in authentication transactions. To address the challenge of information leakage, [13] introduced a Blockchain-enabled accountability framework for content sharing in vertical industry services. This mechanism ensures the secure generation and sharing of watermarked content between clients and service providers. In [14], the authors proposed a Blockchain-based deduplicate data auditing architecture to reduce the workload on service providers and users, alleviating issues related to high costs, repeated data audits, and reliance on third parties. In response to the challenge of malware using Domain Generation Algorithms (DGAs) to steal private information, [15] presented a method for detecting malicious domain names through the extraction and analysis of features using deep neural networks.

In a series of studies, various authors proposed innovative solutions and frameworks. In [16], an efficient attribute-based access control framework was introduced to protect access subject privacy during decision-making using a state-of-the-art hash-based binary search tree. In [17], a secure dispatching approach based on Blockchain technology was presented to enhance the stability of the high-energy power system's distribution network. Additionally, [18] delved into the study of a LEACH protocol combined with a Levenberg-Marquadt Neural Network to assess network lifetime and intrusion detection systems in wireless sensor networks. In [19], a secure link was established in a multi-antenna transmittance environment, even when the Channel State Information (CSI) of an Eavesdropper attack remained anonymous to network users. To ensure secure communication and proper authentication in an IoV scenario, [20] proposed a lightweight mutual authentication mechanism through cryptographic operations, reducing associated costs [21]. A state-of-the-art Road Side Unit (RSU)-based authentication framework for VANETs was introduced in [22], providing a novel solution for securing vehicle-to-vehicle communications.

In a diverse array of research endeavours, authors explored innovative approaches and solutions. In [23], they delved into the development of a game theory-based reputation system designed for scenarios where promises and threats are typically untrustworthy. Meanwhile, in [24], the authors proposed a Blockchain-based system, leveraging the Ethereum blockchain platform, to verify individuals' experience, criminal backgrounds, and educational records as part of the recruitment process. In [25], a comprehensive analysis was conducted, examining the integration of IoT with wireless sensor networks and global-scale internet connectivity, while also addressing challenges related to efficiency, reliability, and sustainability in implementing these applications. In [26], an optimization framework was presented, targeting the reduction of challenges associated with optimizing broadcast parameters and enhancing the physical layer's security in wireless multi-node communication networks. In [27], the authors investigated IoT's energy efficiency and D2D (Device-to-Device) communications with the assistance of an underlying relay technique, aimed at mitigating interference in cellular communications. In a different domain, [28] introduced a framework for intrusion detection within an energy-efficient sensor network through the application of a neuro-fuzzy approach. Privacy and security challenges were also addressed by many renowned authors who proposed various identity-based privacy-preserving authentication methods. In [29], an analysis was presented regarding privacy and security

concerns related to Unmanned Aerial Vehicles (UAVs), along with potential measures to mitigate these concerns.

3. Proposed Work

The main objective of this study is to demonstrate the potential benefits of implementing a Layered CIA (Confidentiality, Integrity, and Authenticity) and blockchain infrastructure in IoV networked devices. The proposed multi-layer framework suggests categorizing the IoV network into three distinct layers. In Layer 1, centralized vehicle communication and RSUs serve as the cluster head for regional clusters comprising vehicles in specific locations. Layer 2 includes RSUs and Controller nodes, which function as cluster heads and miner nodes for lower-layer nodes. Layer 3 encompasses cloud storage and controller nodes. It's essential to note that while RSUs engage in centralized communication with vehicles, they also communicate with other controller nodes and RSUs through local blockchains. Their roles span both Layer 1 and Layer 2 nodes. Layer 2 nodes can securely transact within the blockchain through lightweight consensus mechanisms, executing a locally enabled hyperledger fabric blockchain. Similarly, controller nodes act as intermediaries, connecting cloud storage through the global blockchain and Layer 2 nodes through the local blockchain, as shown in Figure 1. Figure 2 presents the data flow.

In accordance with Algorithm 1, we conducted validation of a list of neighbours, each contributing a node to the blockchain network. In this context, each pair of nodes is tasked with computing the initial point of interaction. Hence, these nodes serve in dual roles, operating as both Layer 2 and Layer 3 nodes. The implementation of stringent security regulations at the high-level layers and the integration of the global blockchain ensure the highest level of anonymity and user security. It is assumed that all controller nodes, vehicle nodes, and cluster heads have a reliable 5G cellular connection. To facilitate the decentralized blockchain techniques at Layers 2 and 3, both controller nodes and RSUs possess sufficient processing capabilities with dedicated servers and CPUs, complementing the existing robust architecture of the cloud storage resources.

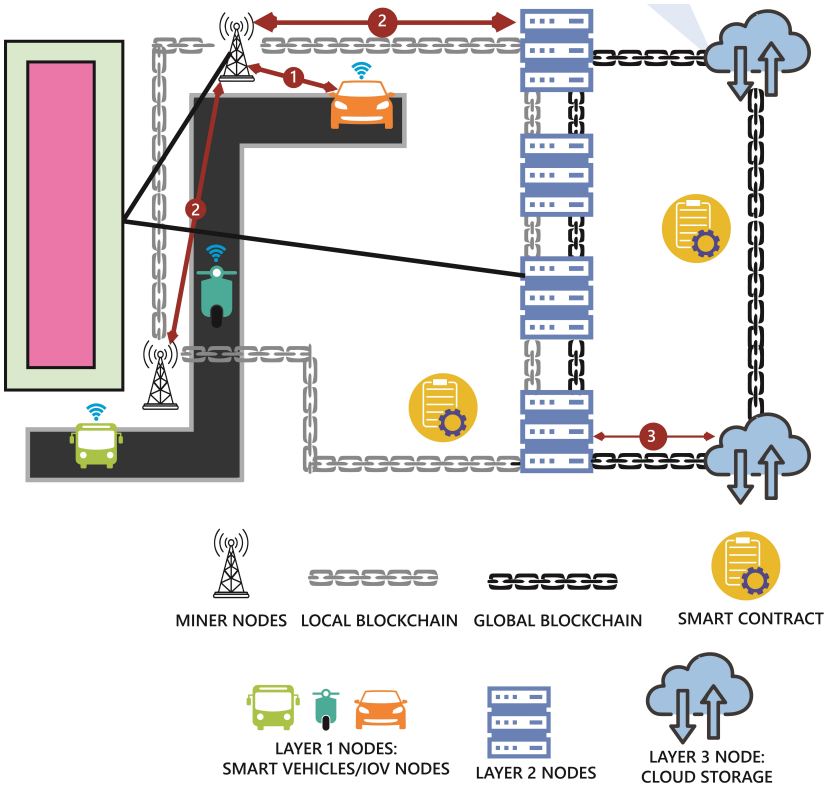

Figure 1: The Proposed Multi-layer Framework

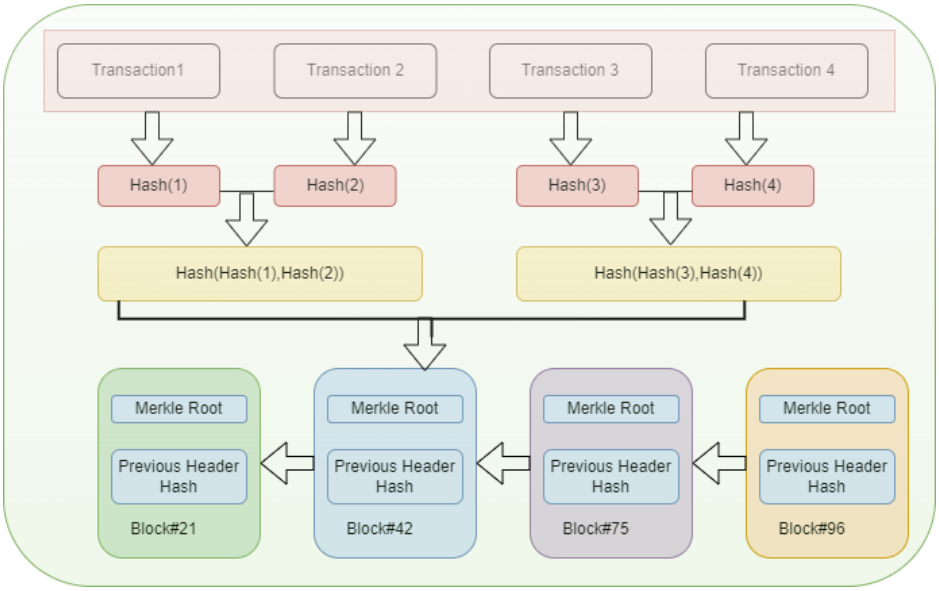

Figure 2: The Proposed Block Transaction

Algorithm 1 BC Network Neighbours Validated

function: safeNodeBC(i, N)
output: Validated Neighbours
procedure:

$adj.n_*[i].node \leftarrow$ create an empty sorted list of adjacency nodes
for each j in $n_* \in N$, where $* = 1, \ldots, n$ and $j \neq i$ **do**
    $t_{i,j}^{p_1} \leftarrow$ Calculate the first point of time for communication
    if $t_{i,j}^{p_1} == t_{i,j}^{p_{\max}}$ and $T_{e^{x_i}}^{i} == T_{e^{x_j}}^{j}$ **then**
        $P_{i,j}^{A}(t) = 1$
        $P_{\sigma i}^{C}(t, N) = P_{\sigma i}^{C}(t, N \setminus \{j\})$
        $T_{(i,j)}^{A} = T_{(i-1,j-1)}^{A} \{\{i, j\}\}; \forall i \neq j$
    else
        $P_{(i,j)}^{A}(t) = 0$
$P_{\sigma i}^{C}(t, N) = P_{\sigma i}^{C}(t, N)$
$T_{(i,j)}^{A} = T_{(i-1,j-1)}^{A}$
return $adj.n_*$

Figure 3 illustrates the network topology, depicting the relational struc-

ture among the nodes, while Figure 4 showcases the proposed framework with interconnected blockchains equipped with Physical Unclonable Functions (PUFs) [30]. These blockchains are connected over the Internet, with an RSU serving as the cluster head within a regional cluster. To ensure the security of every communication, a session key is employed. This session key is a unique key with a specific ID and a defined validity period. Secure communication entails the use of cryptographic keys for processes such as encryption, decryption, and message verification.

Authentication services within the Hyperledger network are provided by a Membership Service Provider (MSP), which also handles duel game authentication services. The MSP takes responsibility for all cryptographic methods and mechanisms employed in the issuance and authentication of users and certificates.

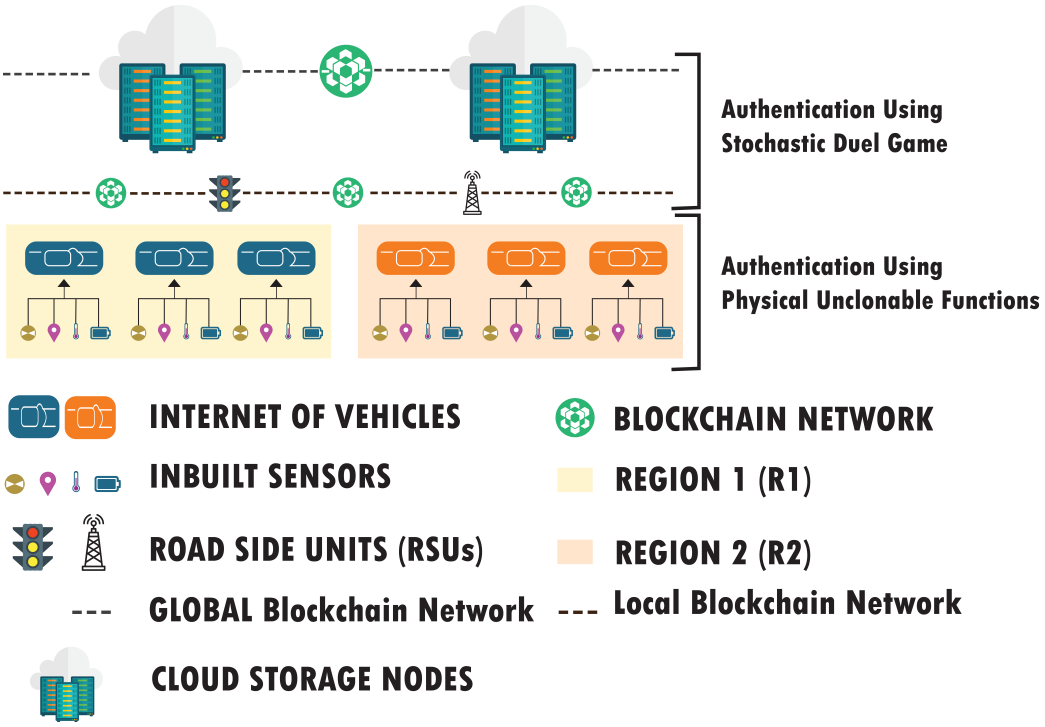

Figure 3: Relational Structure among Network Components with Authentication mechanism

The MSP plays a crucial role in verifying the identification of nodes within

the Hyperledger network. The Hyperledger protocol is efficiently governed by organizations, which oversee network members through MSP. Dedicated or private channels are employed to establish connections between various segments of the network, facilitating interactions. Committers are responsible for confirming and updating the shared ledger. Transactions, utilized for data gathering and transfer, form the foundation of the Hyperledger Blockchain. Smart contracts are used to define transaction terms. In some peer-to-peer communications, the ordering cluster manages queue orders and interactions. The ordering service is responsible for creating transactions and broadcasting them alongside messages. Several factors, such as network topology, influence the assignment of vehicles within the blockchain network as committers or endorsers.

In Layer 3, the controller nodes take on the role of administrators for specific RSUs, akin to how a cloud server operates. These controller nodes oversee devices, respond to queries, and generate data. While the credible nodes in this layer possess significant computing capabilities, they have limitations in processing power. To address this, the global blockchain is employed to introduce more secure asymmetric cryptography algorithms in this layer. Data integrity is guaranteed through a blockchain-based system that prioritizes security and privacy [31].

In the upper layers, there is no central node, and devices maintain data independence. Transactions between nodes at this level are recorded in the blockchain network. Blockchain-based communications with certificates facilitate interactions between computational edge nodes and controller nodes. Smart contracts manage certification distribution within the blockchain, establishing a secure connection among the layer's nodes. It's essential for controller nodes to sign the certificates. Through a blockchain-based approach, both controller nodes and connected cloud storage can collaborate to instil greater confidence in the entities involved. When controller nodes interact with other nodes within independent clusters, trust levels increase.

During the updating of the global and local blockchains, special consideration is given to potential anomalies that could arise due to a swift computational attacker leveraging the duel game framework. To address this, all global and local nodes contributing to the blockchain networks must authenticate their neighbours using Algorithm 2, which maintains a list of these neighbours.

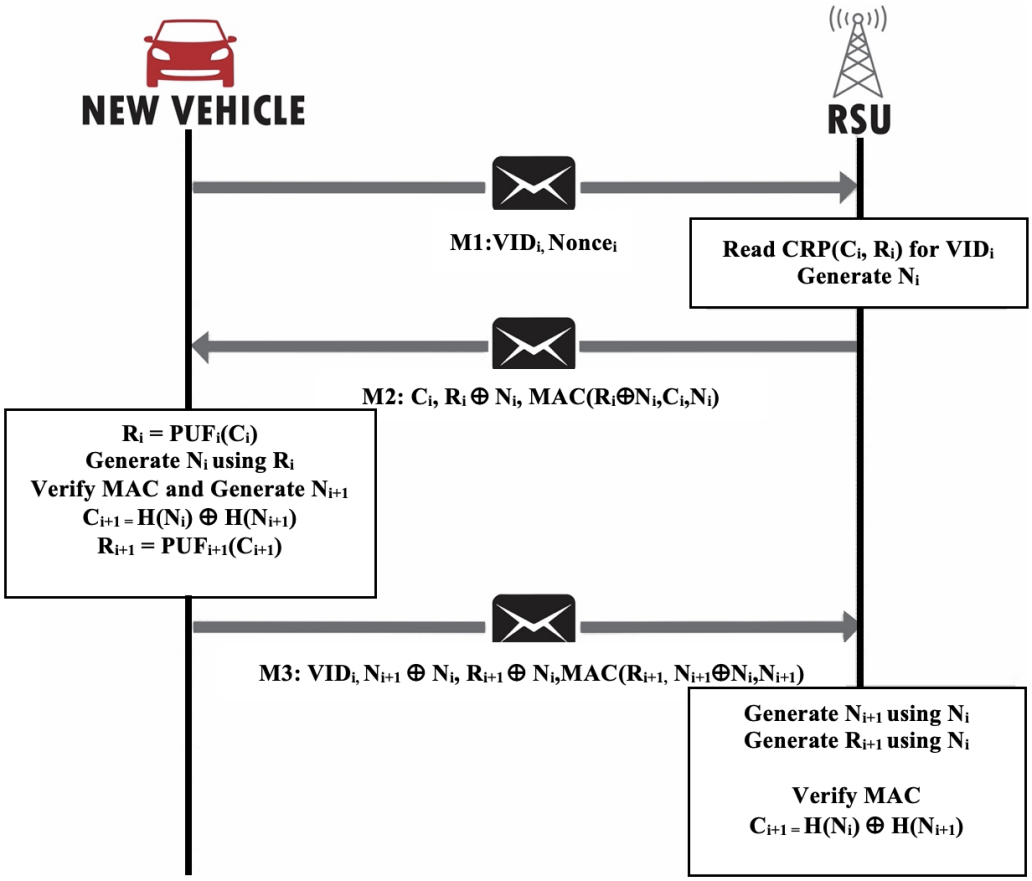

Figure 4: Authentication With Physical Unclonable Functions

4. Experimental Results

4.1. Simulation Scenario

Algorithm 2 illustrates the simulation of the proposed model, which involves a set of RSU nodes denoted as R and a set of vehicles represented as v. At the initialization stage, each vehicle node possesses its individual blockchain account and utilizes contracts for communication with other nodes. Importantly, all RSU nodes maintain a synchronized blockchain snapshot with their peers.

Throughout the lifecycle of the process, as interactions are transmitted, the algorithm demonstrates the information flow pattern that vehicles employ

to interact with the contract. This contract, in turn, connects with the blockchain through RSUs.

Algorithm 2 Framework Simulated

while simulation **do**
  for $i \in r^*, r^* \in R$ for all $* = 1, 2, 3, ..., n$ **do**
    Call Algorithm 1
    for j in i **do**
      $xi * [j].node \leftarrow$ compile contract
      $xi * [j].node \leftarrow$ deploy
      for i in $v*, v* \in V$ for all $* = 1, 2, 3, ..., n$ **do**
        Call Equation1
    Update Network
    for i in $x^*, x^* \in (v^*, r^*)$ **do**
      for j in $adj.m*, m_* \in N$ for all $* = 1, 2, 3, ..., n$ **do**
        if Algorithm1(new$_v$) **then**
          Call Equation1
          $contract \leftarrow$ sendMessage() $\leftarrow v^*[i].node$
          $r * [j].node \leftarrow contract \leftarrow v^*[i].node$
          while msgrequest$(v^*[i].node) == 1$ **do**
            for k in $v^*, v^* \in V$ for all $* = 1, 2, 3, ..., n$ **do**
              if $v^*[k]$.cert == true **then**
                $v * [k]$.cert $\leftarrow$ Permission
                Generate $v * [k]$.ID
                for m in k **do**
                  $vi * [m]$.node $\leftarrow$ compile contract
                  $vi * [m]$.node $\leftarrow$ deploy
                  $vi * [m]$.predecessor = null
                  $vi*[m]$.node.successor = reg_veh.find_suc(v)
                  $sp = \{vk * [m]$.predecessor, $vk * [m]$.node.successor$\}$
                  if $sp \in (v, vk * [m]$.node.successor$)$ **then**
                    $sp = vk * [m]$.node.successor

$$\min r_\mu = \sum_{r \in R} r_\iota r_t \left[1 + \left(\frac{r_\iota}{r_c}\right)^{r_q}\right] \Big/ T_{xN} \tag{1}$$

The detailed information on the parameters utilised in the simulation is

shown in Table 1.

Table 1: Parameters Considered for Simulation

Parameter	**Year**
Speed of the Vehicle	10 – 80 km/hr
Number of Vehicles	1100
Communication Range of the Vehicles	400 m
Communication Range of the RSUs	1100 m
Routing Protocol used	AODV
The Simulation Time	1100 seconds
Wireless Protocol used	802.11a
Area covered	12 km^2

4.2. Performance Analysis

a. **Initial Setup**

To demonstrate the practicality of the proposed blockchain framework, we conducted simulation experiments in three different contexts associated with each layer in the network. In Layer 1, the implementation comprises two parts. The first part involves the authorization and registration of new vehicles using the Physical Unclonable Function (PUF) paradigm. The second part involves connecting to a blockchain network structured through Chord. In Layer 2, RSUs, APIs, and controller nodes are executed. In Layer 3, the deployment simulator for the global blockchain compares Hyperledger Fabric and Ethereum metrics.

The registration of the cluster head begins with the first stage, implemented in Java, followed by the execution of the PUF framework in Matlab. This framework allows clients to become authorized through the cluster head. Node.js is then used to operate the client and server entities, while Python is employed for the peer and client components. Privileged vehicles within the Chord ring can communicate with each other using the peer network. In the Chord framework, each node is aware of its successors and predecessors. A Vehicle ID (VID) is generated for every vehicle upon joining the Chord network. For new nodes to enter the ring, they must initially communicate with active nodes and select their successors. To avoid linear search, each node must maintain a name table with 'i' entries, where 'i' represents the

bit length of the hash keys. The nth node in the network identifies a descendant for the entry of node 'x' as $((x + 2^n - 1) mod c)$, where 'c' represents the Chord ring size and ensures nodes efficiently find their successors or predecessors based on network location. Nodes that have recently joined the network and nodes that fail or leave are managed by the Chord protocol. Node descendant pointers are monitored using a basic stabilization process to ensure the accuracy of query execution during lookups. The entries in the name table are swiftly and accurately verified and updated through the pointers to the descendants. If nodes are removed from the Chord ring due to failures, a lookup initiated before the stabilization is completed can exhibit one of three behaviours. In the first scenario, which is the most accurate, lookups take O(log n) steps to identify the true successor within all name table entries. In the second scenario, there are valid descendant pointers but incorrect names, resulting in accurate lookups that take slightly more time. In the third scenario, regional nodes may have incorrect keys or successor pointers that have not yet transitioned to the newly joined nodes, leading to a failed lookup.

It is important to note that vehicles are assumed to have PUFs linked to CRPs in Layer 1 of the network. Solidity, a language for smart contracts, was used to create the enforcer contract. Python v.3.7.3 was employed to develop the dPoW (delegated Proof of Work) consensus framework and establish the network structure of the IoV-blockchain. The integrated programming environment Remix, designed for Solidity, was used in writing and constructing the smart contract. Additionally, a small amount of web3.js was used for the vehicle nodes and RSUs. Web3.js provides a set of libraries for interacting with an Ethereum node via HTTP, WebSocket, or IPC protocols.

b. **Framework Evaluation**

Omnet++ simulations were employed to evaluate the time overhead and energy usage of controller nodes and RSUs. In the branched blockchain, RSUs were identified as the most resource-intensive components, while in the local blockchain, controller nodes exhibited the highest energy consumption due to their role in processing interactions, executing numerous asymmetric and symmetric encryption, and hashing functions. Among the Layer 1 vehicles, symmetric encryp-

tion emerged as the most computationally demanding function, with the majority of vehicles capable of executing this function. To assess the framework's overhead, it was compared to a baseline method with identical transaction flow but requiring no encryption, ledger, or hashing. In the simulations, IPv6 served as the primary communication framework to meet resource limits.

The RSUs collected data from 15 z1-mote sensors within a 20-second interval, which was mimicked for the vehicles. The results were averaged over approximately five minutes of simulation time. A controller node, directly connected to RSUs, stored the data and then transferred it to the cloud via another controller node, providing a comprehensive understanding of the system's operations. Two distinct traffic flow patterns for stored transactions were simulated. In the first scenario, cloud storage was regularly backed up by vehicles. In the second scenario, data was stored by a vehicle after receiving a query from another network vehicle. Table I presents detailed information regarding the parameters utilized in the simulation.

Additional evaluation criteria encompass the overall packet overhead and the percentage of successful assaults and attacks [32, 33]. In the worst-case scenario, a credible controller node with a substantial block history and high trust level generates a new block containing a single fraudulent transaction. A successful attack occurs when the forged block remains undetected by honest and trustworthy RSUs and controller nodes throughout the twenty simulations. Compared to a baseline where the constructed overlay network resembles Ethereum, the proposed framework exhibits reduced packet overhead.

Figures 5 and 6 depict the results of energy usage, and Figure 7 illustrates the energy comparison with existing cutting-edge research. The proposed framework primarily consumes energy for three fundamental operations: CPU usage, packet listening, and packet transmission. Due to the additional hashing and encryption requirements, the suggested framework generates longer packets, resulting in a twofold increase in energy consumption for transmission. It's worth noting that our analysis assumes that the radio is never turned off. If the radio is intermittently switched off to conserve energy, the relative listening overhead would increase.

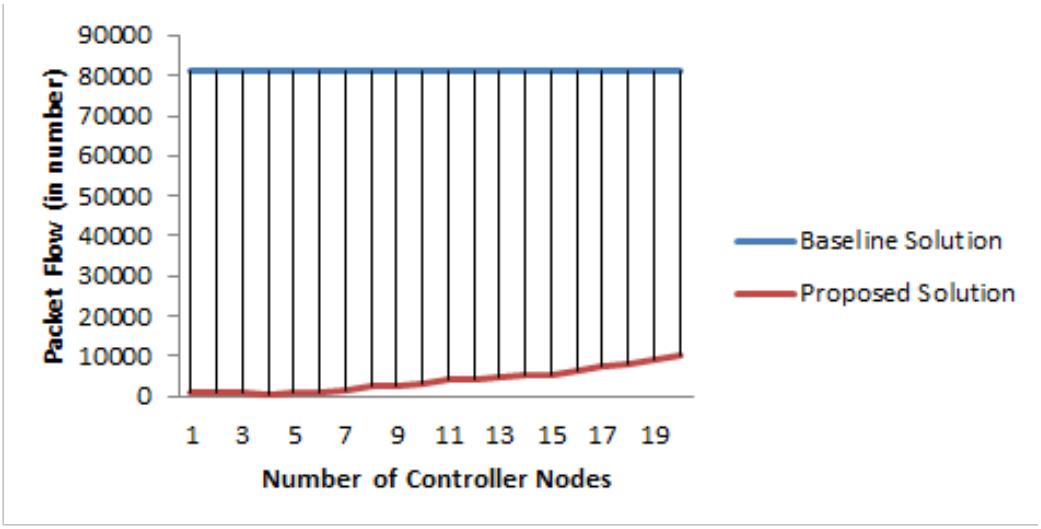

Figure 5: Packet flow comparison with baseline w.r.t. controller nodes for 1500 vehicles

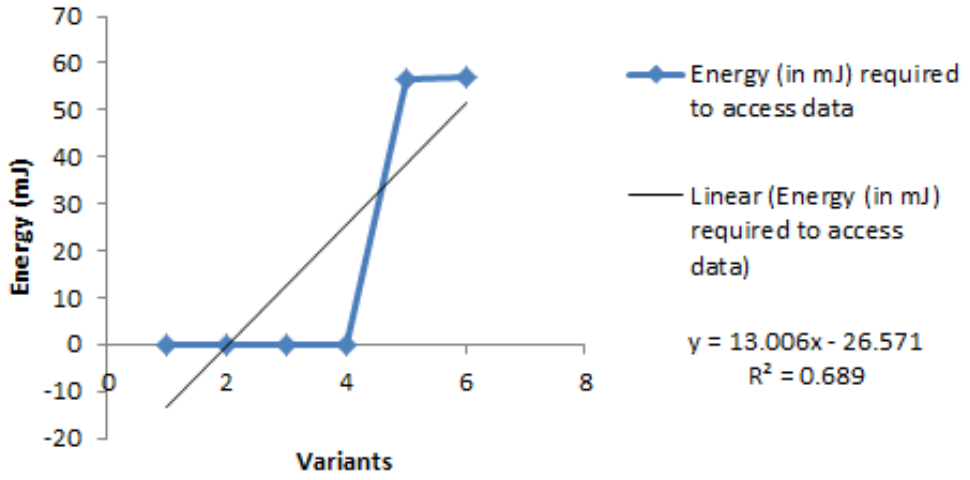

Figure 6: Energy usage for Packet flow comparison with baseline w.r.t. controller nodes for 1500 vehicles

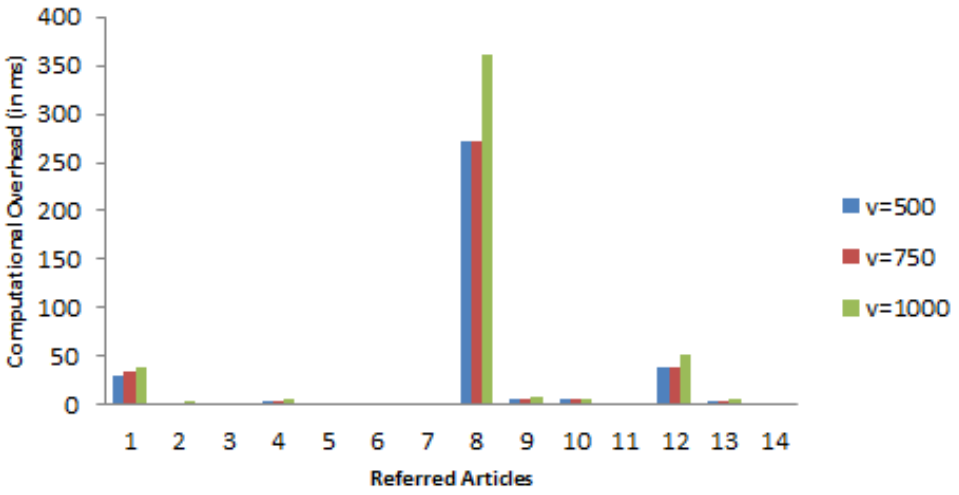

Figure 7: Computation Overhead Relative Comparison

5. Conclusion and Future Work

The self-organization and transparency of the Internet of Vehicles (IoV) make it susceptible to malicious attacks and assaults. This paper presents a game theory-based blockchain authentication method to enhance IoV security. It employs Physical Unclonable Functions (PUFs), a delegated Proof of Work (dPOW) consensus mechanism, and duel gaming to ensure vehicle authentication from the initial entry to movement across different regions without delay. The framework's credibility is reinforced through a Confidentiality, Integrity, and Authenticity (CIA) security analysis. A rigorous examination reveals that, when compared to existing competing systems, the proposed method offers superior functionality, enhanced security, improved communication, and reduced computational costs.

This paper contributes in three significant ways. First, it introduces an enhanced security mechanism based on duel gaming authentication, blockchain, and PUFs. Second, it introduces a lightweight, physical-layer-compatible "branched blockchain" that evolves into a local blockchain aligned with Hyperledger Fabric (HLF) in Layer 2 and a global blockchain based on Ethereum in Layer 3. Third, it addresses side channel and physical cloning attacks. The duel game-based authentication technique proposed here can potentially provide a robust defense against future quantum computing challenges, in addition to the use of lattice cryptography.

While the integration of the Internet of Things (IoT) with IoV offers a wide range of applications, it also presents numerous challenges related to privacy, security, and human-device interfaces. Dealing with the diversity and volume of data, the absence of standardized designs, and scalability issues are among the challenges faced by IoV. Reducing latency and increasing bandwidth are essential for the network's structure.

Funding

No funding was obtained for this study.

Competing interests

There are no competing interests.

Ethical Approval and Consent to participate

The research has consent for Ethical Approval and Consent to participate.

Consent for publication

Consent has been granted by all authors and there is no conflict.

Availability of supporting data

The supporting data can be provided on request.

Authors' contributions

Conceptualization by Celestine Iwendi and Tai Hai; Methodology by Muammer Aksoy; Software by Muammer Aksoy and Senthilkumar Mohan; formal analysis by Tai Hai and Senthilkumar Mohan; Investigation by Ebuka Ibeke and Celestine Iwendi; Resources and data collection by Tai Hai, Senthilkumar Mohan; Writing by: Tai Hai, Muammer Aksoy and Ebuka Ibeke; Validation by: Ebuka Ibeke, Senthilkumar Mohan and Celestine Iwendi. All authors have read and agreed to the published version of the manuscript.

Acknowledgement

We would like to thank anonymous reviewers for their useful suggestions.

References

[1] T. Mezair, Y. Djenouri, A. Belhadi, G. Srivastava, J. C.-W. Lin, Towards an advanced deep learning for the internet of behaviors: Application to connected vehicles, ACM Transactions on Sensor Networks 19 (2) (2022) 1–18.

[2] W. Liang, J. Long, T.-H. Weng, X. Chen, K.-C. Li, A. Y. Zomaya, Tbrs: A trust based recommendation scheme for vehicular cps network, Future Generation Computer Systems 92 (2019) 383–398.

[3] Y. Djenouri, A. Belhadi, D. Djenouri, G. Srivastava, J. C.-W. Lin, A secure intelligent system for internet of vehicles: Case study on traffic forecasting, IEEE Transactions on Intelligent Transportation Systems.

[4] L. Alouache, N. Nguyen, M. Aliouat, R. Chelouah, Survey on iov routing protocols: Security and network architecture, International Journal of Communication Systems 32 (2) (2019) e3849.

[5] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, M. Wen, Mbid: Micro-blockchain-based geographical dynamic intrusion detection for v2x, IEEE Communications Magazine 57 (10) (2019) 77–83.

[6] W. Wu, Z. Yang, K. Li, Internet of vehicles and applications, in: Internet of Things, Elsevier, 2016, pp. 299–317.

[7] A. Yazdinejad, E. Rabieinejad, T. Hasani, G. Srivastava, A bert-based recommender system for secure blockchain-based cyber physical drug supply chain management, Cluster Computing (2023) 1–15.

[8] X. Li, J. Ma, W. Wang, Y. Xiong, J. Zhang, A novel smart card and dynamic id based remote user authentication scheme for multi-server environments, Mathematical and Computer Modelling 58 (1-2) (2013) 85–95.

[9] M. Gupta, B. Sharma, A. Tripathi, S. Singh, A. Bhola, R. Singh, A. D. Dwivedi, n-player stochastic duel game model with applied deep learning and its modern implications, Sensors 22 (6) (2022) 2422.

[10] M. S. Sheikh, J. Liang, W. Wang, Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey, Wireless Communications and Mobile Computing 2020.

[11] X. Li, Y. Xiong, J. Ma, W. Wang, An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards, Journal of Network and Computer Applications 35 (2) (2012) 763–769.

[12] Y. Xu, J. Ren, Y. Zhang, C. Zhang, B. Shen, Y. Zhang, Blockchain empowered arbitrable data auditing scheme for network storage as a service, IEEE Transactions on Services Computing 13 (2) (2019) 289–300.

[13] Y. Xu, C. Zhang, Q. Zeng, G. Wang, J. Ren, Y. Zhang, Blockchain-enabled accountability mechanism against information leakage in vertical industry services, IEEE Transactions on Network Science and Engineering 8 (2) (2020) 1202–1213.

[14] Y. Xu, C. Zhang, G. Wang, Z. Qin, Q. Zeng, A blockchain-enabled deduplicatable data auditing mechanism for network storage services, IEEE Transactions on Emerging Topics in Computing 9 (3) (2020) 1421–1432.

[15] Y. Xu, X. Yan, Y. Wu, Y. Hu, W. Liang, J. Zhang, Hierarchical bidirectional rnn for safety-enhanced b5g heterogeneous networks, IEEE Transactions on Network Science and Engineering 8 (4) (2021) 2946–2957.

[16] Y. Xu, Q. Zeng, G. Wang, C. Zhang, J. Ren, Y. Zhang, An efficient privacy-enhanced attribute-based access control mechanism, Concurrency and Computation: Practice and Experience 32 (5) (2020) e5556.

[17] Y. Xu, Z. Liu, C. Zhang, J. Ren, Y. Zhang, X. Shen, Blockchain-based trustworthy energy dispatching approach for high renewable energy penetrated power systems, IEEE Internet of Things Journal.

[18] M. Mittal, C. Iwendi, S. Khan, A. Rehman Javed, Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using levenberg-marquardt neural network and gated recurrent unit for intrusion detection system, Transactions on Emerging Telecommunications Technologies 32 (6) (2021) e3997.

[19] J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo, W. S. Alnumay, A secure multiuser privacy technique for wireless iot networks

using stochastic privacy optimization, IEEE Internet of Things Journal 9 (4) (2021) 2566–2577. doi:10.1109/JIOT.2021.3050755.

[20] H. Vasudev, V. Deshpande, D. Das, S. K. Das, A lightweight mutual authentication protocol for v2v communication in internet of vehicles, IEEE Transactions on Vehicular Technology 69 (6) (2020) 6709–6717.

[21] T. Hai, D. Wang, T. Seetharaman, M. Amelesh, P. Sreejith, V. Sharma, E. Ibeke, H. Liu, A novel & innovative blockchain-empowered federated learning approach for secure data sharing in smart city applications, in: International Conference on Advances in Communication Technology and Computer Engineering, Springer, 2023, pp. 105–118.

[22] M. Bayat, M. Pournaghi, M. Rahimi, M. Barmshoory, Nera: A new and efficient rsu based authentication scheme for vanets, Wireless networks 26 (5) (2020) 3083–3098.

[23] B. Polak, ECON 159 - Lecture 16 - Backward Induction: Reputation and Duels — Open Yale Courses.
URL https://oyc.yale.edu/economics/econ-159/lecture-16

[24] S. Rathor, A. Agrawal, A robust verification system for recruitment process by using blockchain technology, International Journal of Blockchains and Cryptocurrencies 1 (4) (2020) 389–399.

[25] K. Bajaj, B. Sharma, R. Singh, Integration of wsn with iot applications: a vision, architecture, and future challenges, in: Integration of WSN and IoT for Smart Cities, Springer, 2020, pp. 79–102.

[26] J. H. Anajemba, Y. Tang, C. Iwendi, A. Ohwoekevwo, G. Srivastava, O. Jo, Realizing efficient security and privacy in iot networks, Sensors 20 (9) (2020) 2609.

[27] J. H. Anajemba, Y. Tang, J. A. Ansere, C. Iwendi, Performance analysis of d2d energy efficient iot networks with relay-assisted underlaying technique, in: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2018, pp. 3864–3869. doi:10.1109/IECON.2018.8591373.

[28] M. Mittal, L. K. Saraswat, C. Iwendi, J. H. Anajemba, A neuro-fuzzy approach for intrusion detection in energy efficient sensor routing, in: 2019

4th International conference on internet of things: Smart innovation and usages (IoT-SIU), IEEE, 2019, pp. 1–5. doi:10.1109/IoT-SIU.2019.8777501.

[29] M. A. Siddiqi, C. Iwendi, K. Jaroslava, N. Anumbe, Analysis on security-related concerns of unmanned aerial vehicle: attacks, limitations, and recommendations, Mathematical biosciences and engineering 19 (3) (2022) 2641–2670. doi:10.3934/mbe.2022121.

[30] W. Wang, Q. Chen, Z. Yin, G. Srivastava, T. R. Gadekallu, F. Alsolami, C. Su, Blockchain and puf-based lightweight authentication protocol for wireless medical sensor networks, IEEE Internet of Things Journal 9 (11) (2021) 8883–8891.

[31] E. A. Mantey, C. Zhou, V. Mani, J. K. Arthur, E. Ibeke, Maintaining privacy for a recommender system diagnosis using blockchain and deep learning., Human-centric computing and information sciences 13 (47). doi:https://doi.org/10.22967/HCIS.2023.13.047.

[32] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking, Computers & Security 88 (2020) 101629.

[33] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, H. Hu, F. Gong, Achieving reliable and secure communications in wireless-powered noma systems, IEEE Transactions on Vehicular Technology 70 (2) (2021) 1978–1983. doi:10.1109/TVT.2021.3053093.