[1]Peng Liu
[2]Yinghui Xu
[3]Yanqing Wang
[4,*]Ping Fan

A Blockchain Empowered Smart Home Access Scheme Based on Zero-trust Architecture

JES Journal of Electrical Systems

Abstract: - The rapid popularity of smart home devices worldwide has brought a lot of convenience to people's lives and spawned numerous new applications. However, it has also elevated data and privacy security risks in household scenarios to an unprecedented level. In this paper, we propose a device access solution based on a zero-trust network architecture to address the cybersecurity risks in smart home scenarios. The proposed solution utilizes a zero-knowledge identity verification algorithm based on quadratic residues to achieve mutual authentication and authorization between devices and central control without exposing device privacy. To enhance the efficiency of verification and authorization, we introduce an incentive model based on information asymmetric algorithms, distributing a portion of the verification tasks to devices with redundant computing power. By comparing with traditional methods, this solution demonstrates higher security, improved verification efficiency, and optimized allocation of computing resources, all while protecting device privacy.

Keywords: Smart Home, Zero Trust Architecture, Trustworthy Access, Blockchain, Cyber Security.

I. INTRODUCTION

A. Background

With the rapid development of the Internet of Things (IoT) industry, smart homes, as an important application scenario of IoT technology, are gradually becoming a part of people's lives, bringing convenience, comfort, and security to households worldwide. Smart homes not only provide users with a new home experience but also play a significant role in the construction of smart cities and energy conservation.

Currently, the smart home industry is in a stage of vigorous growth. According to data released by IDC, global smart home device shipments continued to increase from 2017 to 2021. Despite the impact of the COVID-19 pandemic in 2020, global smart home device shipments still maintained growth, reaching a growth rate of 11.7% in 2021. By 2022, the global smart home market reached 110 billion USD, with shipments totaling 874 million units [1]. Currently, smart home products have a higher penetration rate in developed regions such as Europe, America, Japan, and South Korea. However, with the increasing number of global internet users and the growth of disposable income for consumers in developing economies, the smart home market is expected to further expand. According to research by Fortune Business Insights, the global smart home market is expected to surpass 150 billion USD in 2025, with a projected compound annual growth rate of 20.1%. By then, the number of smart home devices is expected to account for approximately 20% of the total number of IoT connections worldwide [2].

B. Challenges

However, the smart home industry also faces some challenges. Classified by functions, smart homes include eight major modules: entertainment system, security system, control system, lighting system, kitchen and bathroom appliances system, network and communication system, health and medical system, and indoor environment system. The defense strategies of these modules vary, and there is a lack of unified security standards. The interconnection between various devices and systems has narrowed the security boundaries of smart homes, and end-users without professional network security knowledge may face significant data and privacy security risks. According to the experiment conducted by the UK consumer organization "Which?" in collaboration with the Global Cyber Alliance (GCA), the installed smart home products experienced over 12,000 scans and network attacks within a week [3], severely impacting consumer trust in smart homes.

Zero Trust Architecture (ZTA) is a new security concept with the core principle of "never trust, always verify," aiming to address potential threats from a dynamic network environment by conducting appropriate checks at all interfaces and endpoints [4]. ZTA is suitable for network environments where end-to-end trustworthiness cannot

[1] China Electric Power Research Institute, Beijing 100192, China
[2] China Electric Power Research Institute, Beijing 100192, China
[3] China Electric Power Research Institute, Beijing 100192, China
[4] University of Electronic Science and Technology of China, Chengdu 611731, China
*Corresponding author: Ping Fan

be guaranteed, making it a fitting solution for the diverse functionalities and frequent device changes in smart home products. In this paper, based on the ZTA security model, we propose a smart home device access verification method using zero-knowledge proofs and optimize its efficiency with an incentive mechanism based on information symmetry algorithms.

C. Contribution

The main contribution of this paper are as follows:

- We apply a distributed zero-knowledge proof algorithm based on quadratic residues to the device verification process. In this process, a new device generates a random number, encrypts it using quadratic residues, and sends it to multiple verifying devices for legitimacy verification. The verifying devices send the verification result and the hash value of the device key to the central control system, which verifies the device identity again based on the hash value of the device key. During the interaction, the device also verifies the legitimacy of the central control system, achieving interactive verification.
- To improve verification efficiency and reduce computational costs, we establish an incentive mechanism based on information symmetry algorithms. This mechanism allows the central control system to allocate tasks to other smart home devices within its controllable range that have redundant computational power.
- Building a smart home system structure based on 2-level blockchain to improve the efficiency and security.

The rest of the paper is organized as follows: Section 2 reviews existing research on IOTs secure access methods with ZTA. Section 3 introduces the quadratic residues-based encryption algorithm and its application, and proposes an improved solution by integrating the incentive mechanism and blockchain method. Section 4 evaluates its effectiveness by simulation experiments. Section 5 provides a summary and analysis of the evaluation results and discusses the limitations and future research directions of this study.

D. Related Work

Currently, research on security methods based on ZTA is mainly focused on traditional Internet domains, while studies on IoT device security access are mostly related to overall architecture. Jie L et al. explored the feasibility of integrating Fog/edge computing with the Internet of Things, which enables faster response and higher quality of service [5]. D Greenwood proposed a ZTA-based security architecture for energy company information and data security. Test results showed that the architecture effectively protects the IT system of energy companies and reduces the risks faced by sensitive data [6]. Rasheed et al. presented an interactive zero-knowledge proof verification strategy for self-organizing networks, balancing privacy security and computational consumption by considering response speed and privacy information disclosure during network verification [7]. Bhargava et al. proposed a trust evaluation method for vehicular networks, which utilizes trust values of existing vehicles in the network and feedback from surrounding vehicles to assess trust levels and classify the behavior of vehicles accordingly [8]. Samanta H studied the security of IoT applications and proposed a low-cost IoT-based energy optimization management solution, providing personalized security for IoT energy terminals [9].

In summary, current research in the IoT domain mainly focuses on security access related to specific application scenarios, with a focus on overall architecture and strategies. So we introduces the ZTA security architecture into the significant context of smart homes in IoT applications, aiming to contribute practically to this field.

II. CONSTRUCTION OF SMART HOME ACCESS SCHEME BASED ON ZTA

A. System Model

Zero-knowledge proofs are widely used in various fields such as security protocols, authentication, and privacy protection [10]. They allow a prover to demonstrate the truth of a statement to a verifier without revealing any actual information related to that statement, ensuring privacy and security.

In a zero-trust environment, where the identities of the prover and verifier are not fixed, both parties can mutually verify each other. Therefore, employing zero-knowledge proofs in an interactive manner can effectively protect the privacy and security of both the verifier and prover [11]. We will build the structure of the smart home system around zero-knowledge proofs and provide an explanation of our verification algorithm.

B. System Structure

The smart home system mainly consists of products with consumer-level and is still a relatively new area with no unified standards yet [12]. In practice, household smart home systems typically include a central control device (CCD) that allows interactions and serves as the core of the smart home. The smart home system can expand and integrate various types of devices and exchange data with different household appliances around CCD, such as

communication devices, security devices, billing meters, energy-saving devices, or smart furniture [13]. The CCDs will also connect to the cloud of service providers or communities to obtain professional security support.

The proposed trustworthy intervention architecture in this paper includes a main chain and several sidechains. As shown in Figure 1 by solid lines, the main chain is maintained by the more powerful computational CCDs, responsible for recording the devices' factory information and keys. It is managed centrally by professional community network monitoring or service providers in the cloud. The sidechains consist of smart home devices within the service scope of the CCDs, as shown in Figure 1 by dashed lines. The sidechains are mainly responsible for the initial devices authentication and authorization when entering the central control system, record the verification time, which will be referred to when re-verification is needed in future interactions. The tolerance threshold for verification time is recorded by the main chain and synchronized to the sidechains. The information required for identity verification on the sidechains is provided in the form of hash values by the main chain, reducing the information that needs to be recorded on the sidechains.

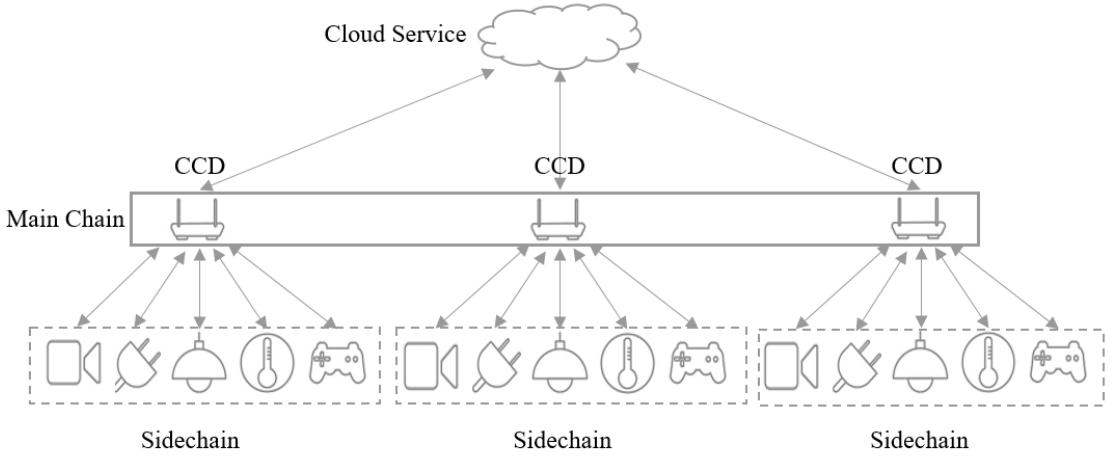

Figure 1: The Structure of Smart Home System in Community

The existence of the main chain and sidechains can meet the requirements of continuous device verification and authorization in a zero-trust network architecture. By utilizing the redundant computational power in the sidechains without affecting their function, optimal allocation of computational resources can be achieved, reducing verification costs and improving verification efficiency. Although this interaction method may cause additional latency, considering the low amount and frequency of smart home device access, as well as privacy protection and low algorithm complexity, this interaction approach still has significant advantages and reliability in household-level smart systems.

C. Verification Algorithm

Before device access, users or suppliers will put the device's label and key information into the target CCD, noted as (TAG, KEY), where TAG contains private data such as the device's serial number or brand ,and KEY is used for encryption. (TAG, KEY) is considered as sensitive information that cannot be revealed. After entering the private information during verification. The backend randomly generates prime numbers (p_1, p_2, p_3, p_4) and stores p_1p_2 and p_3p_4 as public parameters on the main chain and sidechains. New devices will use $(TAG, KEY, p_1p_2, p_3p_4)$ to validate their legitimacy. Now the information on the main chain is $(TAG, KEY, p_1p_2, p_3p_4, p_1, p_2, p_3, p_4)$ and the information on the sidechain is $(p_1p_2, p_3p_4, p_3, p_4)$. We assume the number of available verification devices in the sidechain is I.

Step 1: When a new device is asking for connection, a verification device $i \in I$ is randomly selected, and determines if verification is required based on the verification time from the sidechain. If needed, it notifies other verification devices to start generating verification strategies. Each verification device generates a n-bits random binary number r_i as formula (1) and a random c-dimensional binary vector $\boldsymbol{e_i}$ as formula (2),

$$r_i = \{0,1\}^n,\ r_i \in Z^*_{p_3p_4}, i \in I \tag{1}$$

$$\boldsymbol{e_i} = [e_{i1}, e_{i2} \cdots e_{ic}],\ e_{ij} \in \{0,1\},\ j = 1,2 \ldots c. \tag{2}$$

then sends them to the device awaiting for verification. All message is combined by the new device as $M_1 = .\{r_1, r_2 \cdots r_I,\ \boldsymbol{e_1}, \boldsymbol{e_2} \cdots \boldsymbol{e_I}\}$.

Step 2: The device awaiting verification calculates zero-knowledge evidence based on M_1. It generates a random number $R \in Z^*_{p_3p_4}$ and performs XOR operation to generate $x \in Z^*_{p_1p_2}$ with formula (3).

$$x = KEY \oplus R \oplus r_i\ ,\ i \in I \tag{3}$$

Then calculates the hash values $Hash(R)$ and $Hash(x)$, and encrypts R and x to obtain R^* and X as formula (4) and (5).

$$R^* = R^2\ mod\ p_3 p_4 \tag{4}$$

$$X\ = x^2\ mod\ p_1 p_2 \tag{5}$$

It computes the hash value $H = Hash(TAG||KEY)$ and encrypts it as H^* by formula (6).

$$H^* = (H^2\ mod\ p_1 p_2) \oplus R \tag{6}$$

For each vector $\boldsymbol{e_i}$, it generates a corresponding vector $\boldsymbol{E_i} = \{RH^{e_{i1}}, RH^{e_{i2}} \cdots RH^{e_{ic}}\}$. At last, the device awaiting for verification sends message $M_2 = \{R^*, X, H^*, \boldsymbol{E_i}, Hash(R), Hash(x)\}$ to the corresponding verification devices.

Step 3: The verification devices validate the identity of the newly connected device based on M_2. First, based on the sidechain information (p_3, p_4), R can be solved by solving the following equations (7) using the Cipolla algorithm to obtain four solutions for R.

$$\begin{cases} R^2 \equiv R^* mod\ p_3 \\ R^2 \equiv R^* mod\ p_4 \end{cases} \tag{7}$$

By comparing the hash values of the four solutions, the value of the random number R can be determined [14]. Then, each verification device calculates the verification result $j_i = \{j_{i1}, j_{i2} \cdots j_{ic}\}$ as formula (8) and sends message $M_3 = \{j_1, j_2 \ldots j_I, M_1, M_2\}$ to CCD.

$$j_{ik} = (RH^{e_{ik}})^2 mod\ p_1 p_2 - R^2 (H^* \oplus R)^{e_{ik}} mod\ p_1 p_2\ , i = 1,2 \ldots I,\ k = 1,2 \ldots c \tag{8}$$

Step 4: The CCD validates the identity of the newly connected device based on M_3. If the device awaiting verification is already legally registered, all values in the $\{j_1, j_2 \ldots j_I\}$ vector will be 0. For the right condition, the CCD can decrypt x based on $X, Hash(x)$ and (p_1, p_2) by formula (9).

$$\begin{cases} x^2 \equiv X\ mod\ p_1 \\ x^2 \equiv X\ mod\ p_2 \end{cases} \tag{9}$$

Similarly as Step 3 , the value of x can be obtained by using the Cipolla algorithm and comparing the hash values. Based on the value of x, we can get KEY value by formula (10).

$$KEY = x \oplus R \oplus r_i\ ,\ i \in I \tag{10}$$

Then we can confirm the legitimacy of identity if the KEY value is the same as in the main chain. After confirmation, $YES = TAG \oplus R \oplus x$ is calculated as evidence and the device's key is updated to $KEY^* = Hash(KEY||R||r_i),\ i \in I$. CCD will send $M_4 = \{BOOL, Hash(YES)\}$ to verification devices, where BOOL means the conclusion of verification.

Step 5: The verification devices update the sidechain based on M_4 and forward $Hash(YES)$ to the newly connected device.

Step 6: The newly connected device validates the legitimacy of CCD by computing $Hash(TAG \oplus R \oplus x)$ and comparing it with $Hash(YES)$. If they are the same, it indicates the legitimacy of the base station, then update the KEY to KEY^* before next identity verification.

The complexity of this verification algorithm mainly depends on the length of the vector $\boldsymbol{e_i}$ generated in Step 1. As c increases, the number of iterations in Steps 3 and 4 increases linearly, resulting in a complexity of $O(c)$. All the steps are shown as Figure 2.

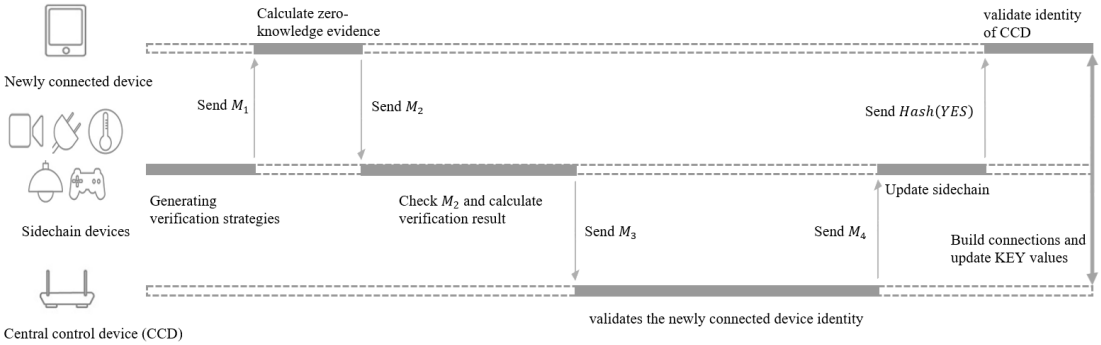

Figure 2: The Process of Verification Algorithm Based on ZTA for Smart Home

Due to the heterogeneous computational capabilities of the components in the smart home system, not all devices in the sidechain may be available when new verification demands arise, leading to information asymmetry between the CCD and the verification devices. To solve this, the CCD can first calculates the probability P_i of

computing power i being available for less than the threshold time T based on historical data, and only selects those with higher probability as candidates [15]. We note the workload as , the utility of using computing power i can be written as following:

$$U_{i,S_i,P_i} = \frac{S_i}{P_i}\pi_i - \alpha_i F_i^2 W \tag{11}$$

Where S_i means the credibility calculated by CCD based on historical data [16], S_i/P_i determines the type of computing power i. α_i is the unit workload cost , π_i is the work reward and F_i is the computation frequency. π_i and F_i are generated by CCD and π_i is positively correlated with F_i. Then the utility of CCD using edge computing power i can be represented as following:

$$U_{CCD}(i) = \frac{S_i}{P_i}\pi_i - \alpha_i F_i^2 W \tag{12}$$

To achieve maximum efficiency, this problem is transformed into a multivariate linear programming problem as formula (13), which can be solved using Lagrange multiplier method [17] to obtain the optimal solution.

$$\begin{cases} max \sum_{i=1}^{I} \varepsilon_i U_{CCD}(i) , \sum_{i=1}^{I} \varepsilon_i = 1 \\ s.t. \;\; U_{i,S_i,P_i} \geq 0; \\ \quad U_{i,S_i,P_i} \geq U_{i,S_j,P_j} , i \neq j \end{cases} \tag{13}$$

D. Security Analysis

Currently, privacy leakage in smart home systems mainly includes malicious access, data interception, and local area network eavesdropping [18]. We will analyze from those scenarios.

For maliciously accessed devices, assuming they have obtained the public parameter $p_1 p_2$ from sidechain, but their evidence x, which calculated using randomly generated keys, cannot be verified by the main chain's key record in Step 4. When the new device performs identity verification, its privacy information is encrypted as $Hash(TAG||KEY)$ and X. During the communication process, this encrypted information may be intercepted through data packet capture. However, since the specific values of the prime factors (p_1, p_2) are unknown, it is still impossible to reverse-calculate the device's private information. During the verification process by the sidechain's device, the interaction information from the CCD is the encrypted. Since the sidechain device does not know the value of (p_1, p_2), it cannot decrypt the KEY value and device label informationTAG. Therefore, local area network eavesdropping will also be ineffective.

E. Simulation

In this section, we use simulation to demonstrate the performance of the verification algorithm. We set the parameter according to [19] as $\alpha_i = 5 \times 10^{-26}$; $F_i = 3 \times 10^9\, Hz$; $W = 10^9$ and the equipment for the simulation experiment is Intel(R) Core(TM) i7-10510U CPU @1.80 GHz RAM 16GB. The result is shown in Figure 3 and Figure 4.

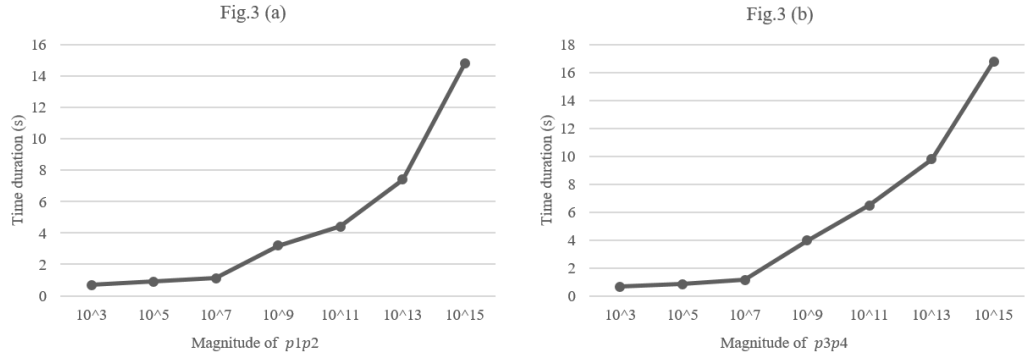

Figure 3: The Time Duration with Different Prime Numbers

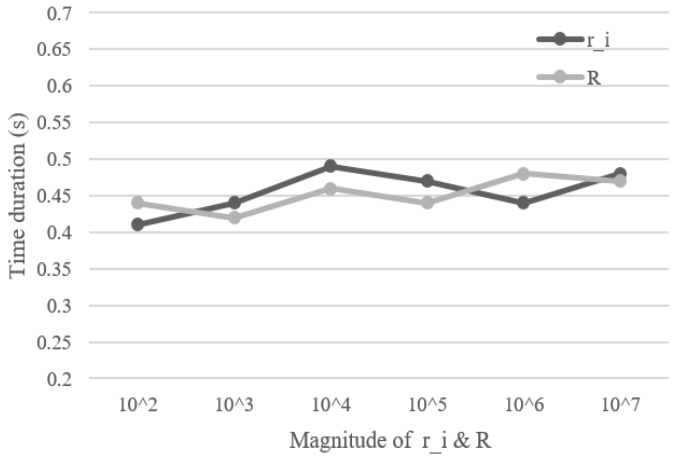

Figure 4: The Time Duration with Different Magnitude of Factors

We can find in Figure 3(a) that as the increase of p_1p_2 , the verification duration increases , which due to the CCD will need p_1p_2 to decrypt the KEY value. The duration is related with the quadratic residues computation workload, which is mod by p_1p_2. Similar result shows in Figure 3(b), the verification duration increases with p_3p_4. It is the same reason as CCD, the sidechain devices and newly connected device will all need p_3p_4 to encrypt or decrypt value R. As in Figure 4, we set the abscissa as magnitude of r_i or R. The ordinate is the verification duration under fixed (p_1p_2 , p_3p_4) , the result shows the duration is slightly effected, because r_i or R are mainly used to calculate residue with much lower computation than quadratic residues.

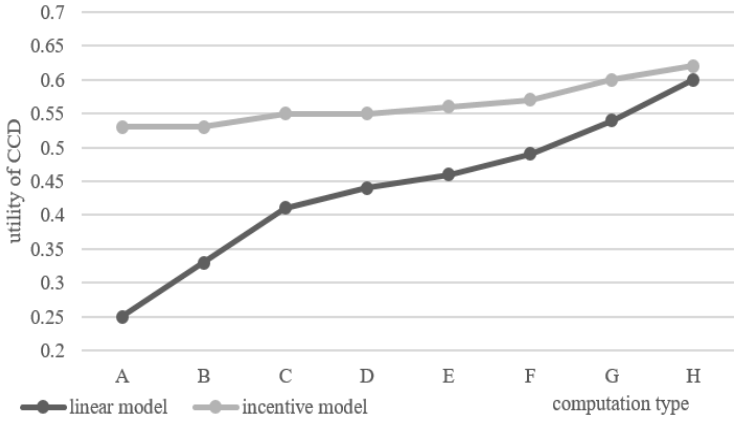

Figure 5: The Utility of CCD with Different Model

In Figure 5 we compare our incentive model of distributing a portion of the verification tasks to devices with redundant computing power with traditional linear model, which assume equally distribute workload to all available units [20]. As we can see, We use the horizontal axis to represent different types of computing power, primarily determined by the formula S_i/P_i in Equation 12, and the vertical axis to represent the utility in that computing power type. The utility of CCD rises as the S_i/P_i value grows, which means stronger willingness. In each kind of computation type, the incentive model based on information asymmetric algorithms is more efficient than the linear one.

III. CONCLUSION

In this paper, we propose a device access solution based on a zero-trust network architecture to address the cybersecurity risks in smart home scenarios. The proposed solution utilizes a zero-knowledge identity verification algorithm based on quadratic residues to achieve mutual authentication between newly connected device and CCD without exposing any privacy information. To enhance the efficiency of verification and authorization, we introduce an incentive model based on information asymmetric algorithms, distributing a portion of the verification tasks to devices with redundant computing power. By comparing with traditional methods, this solution demonstrates higher efficiency of optimizing computing resources and higher security. Due to the fast literation of smart home devices and better user experience, research will focus on how to reduce the verification duration in the future.

REFERENCES

[1] M Moniruzzaman, S Khezr, A Yassine, R Benlamri. "Blockchain for smart homes: Review of current trends and research challenges." Computers & Electrical Engineering 83 (2020): 106585.

[2] Ferreira, Laura, Tiago Oliveira, and Catarina Neves. "Consumer's intention to use and recommend smart home technologies: The role of environmental awareness." Energy 263 (2023): 125814.

[3] Basarir-Ozel, Birgul, Hande Bahar Turker, and Vesile Aslihan Nasir. "Identifying the key drivers and barriers of smart home adoption: A thematic analysis from the business perspective." Sustainability 14.15 (2022): 9053.

[4] Ankur G, Rajesh G,Dhairya J, et al. Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications. Computer Communications, 2023, 206.

[5] Jie L, Wei Y, Nan Z, et al. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications . IEEE Internet of Things Journal, 2017, 4(5).

[6] D Greenwood, "Applying the principles of zero-trust architecture to protect sensitive and critical data", Network Security, vol. 2021, no. 6, pp. 7-9, 2021.

[7] Rasheed, Amar A., Rabi N. Mahapatra, and Felix G. Hamza-Lup. "Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks." IEEE Transactions on Intelligent Transportation Systems 21.2 (2019): 867-881.

[8] A Bhargava, S Verma, BK Chaurasia, GS Tomar. "Computational trust model for Internet of Vehicles." 2017 Conference on Information and Communication Technology (CICT). IEEE, 2017.

[9] H Samanta, A Bhattacharjee, M Pramanik et al., "Internet of things based smart energy management in a vanadium redox flow battery storage integrated bio-solar microgrid", TERI information digest on energy and environment: TIDEE, vol. 20, no. 1, pp. 69-69, 2021.

[10] Peirong L, Wei O, Haozhe L, et al. A zero trust and blockchain-based defense model for smart electric vehicle chargers. Journal of Network and Computer Applications, 2023, 213.

[11] Wylde, Allison. "Zero trust: Never trust, always verify." 2021 international conference on cyber situational awareness, data analytics and assessment (cybersa). IEEE, 2021.

[12] H Touqeer, S Zaman, R Amin, M Hussain, F Al-Turjman, M Bilal. "Smart home security: challenges, issues and solutions at different IoT layers." The Journal of Supercomputing 77.12 (2021): 14053-14089.

[13] Tatarnikova, T., and B. Sovetov. "Smart home security management." Journal of Physics: Conference Series. Vol. 1864. No. 1. IOP Publishing, 2021.

[14] Barreto M L S P, Voloch F J. Efficient Computation of Roots in Finite Fields.. Des. Codes Cryptography, 2006, 39(2).

[15] Haider, Fourat, Wang, et al. Spectral/Energy Efficiency Tradeoff of Cellular Systems With Mobile Femtocell Deployment. IEEE Transactions on Vehicular Technology, 2016, 65(5).

[16] Hao, M., Ye, D., Wang, S., Tan, B., & Yu, R. (2021, April). URLLC resource slicing and scheduling in 5G vehicular edge computing. In 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring) (pp. 1-5). IEEE.

[17] X. Huang, R. Yu, D. Ye, L. Shu and S. Xie, "Efficient Workload Allocation and Use r-Centric Utility Maximization for Task Scheduling in Collaborative Vehicular Edge Compu ting," in IEEE Transactions on Vehicular Technology, vol. 70, no. 4, pp. 3773-3787, April 2021

[18] Ali, Sonny, and Zia Yusuf. "Mapping the smart-home market." Tech. rep (2018).

[19] J Song, PW Harn, K Sakai, MT Sun, WS Ku. "An RFID Zero-Knowledge Authentication Protocol Based on Quadratic Residues." IEEE Internet of Things Journal 9 (2022): 12813-12824.

[20] Z Zhou, H Liao, X Zhao, B Ai, M Guizani. "Reliable Task Offloading for Vehicular Fog Computing Under Information Asymmetry and Information Uncertainty." IEEE Trans. Vehicular Technology 68.9(2019).