

Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing

Seema G. Aarella
University of North Texas
Denton, Texas, USA
seema.aarella@unt.edu

Elias Kougianos
University of North Texas
Denton, Texas, USA
elias.kougianos@unt.edu

Saraju P. Mohanty
University of North Texas
Denton, Texas, USA
saraju.mohanty@unt.edu

Deepak Puthal
Khalifa University
Abu Dhabi, UAE
deepak.puthal@ku.ac.ae

ABSTRACT

Collaborative Edge Computing (CEC) works on the distributed model, and is established at the Fog layer that consists of multiple edge devices like Edge Data Centers (EDCs), Edge Routers etc. In the CEC environment, the Edge layer has the capability of storing and processing data. Since the processing capacity is limited, many edge devices collaborate with each other to offload the processing in a scheme called Load Balancing. CEC enables applications in smart villages through task offloading/sharing, which calls for a trusted security system to make the resource sharing and information safe. Since the Edge is a resource-constrained environment where not all data centers are resourceful enough to implement computation intensive security systems. Physically Unclonable Functions (PUF) are a robust, secure, and light-weight solution for providing hardware security. PUFs are used to authenticate the EDCs during load balancing in a collaborative edge computing environment. Though PUFs are secure and difficult to remodel, the drawback lies in the storage of Challenge-Response Pairs (CRP) in a CRP database. The storage space for the CRP database becomes a concern when many EDCs participate in dynamic load balancing and each EDC needs to store a copy of the database. This research proposes a PUF based certificate Authority protocol for authentication of EDCs which will eliminate the need for CRP database storage while harnessing the security feature of the PUF. Further, in this research the efficiency of the PUF based authentication system is evaluated through theoretical analysis and experimental results.

CCS CONCEPTS

• Security and privacy → Distributed systems security; Hardware-based security protocols; • Networks → Security protocols.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
GLSVLSI '23, June 5–7, 2023, Knoxville, TN, USA

© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 979-8-4007-0125-2/23/06...\$15.00
<https://doi.org/10.1145/3583781.3590249>

KEYWORDS

Collaborative Edge Computing, Edge Load Balancing, Cybersecurity, Security-by-Design (SbD), Hardware Assisted Security (HAS), Physical Unclonable Functions (PUF), Device Authentication, Certificate Authority

ACM Reference Format:

Seema G. Aarella, Saraju P. Mohanty, Elias Kougianos, and Deepak Puthal. 2023. Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing. In *Proceedings of the Great Lakes Symposium on VLSI 2023 (GLSVLSI '23)*, June 5–7, 2023, Knoxville, TN, USA. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3583781.3590249>

1 INTRODUCTION

Authentication is a necessary feature for the different layers of a smart environment. It is needed to prove identities of the devices and to ensure confidentiality. Cryptography is largely used in security solutions for IoT applications, the challenge however lies in providing a lightweight solution, in terms of generating smaller keys in resource constrained environments and, significantly, at the physical layer which involves devices with low processing power. Lightweight security can be provided by hardware as well as software. Edge computing provides speed, reliability, security, scalability, and repeatability, with the ability to process data closer to the IoT (Internet-of-Things) devices. Edge nodes are more vulnerable compared to cloud and hence security and privacy is an area that needs most attention [6]. The edge enables cooperative load sharing/offloading for effective use of computing resources and to reduce latency in time sensitive processes. The task offloading process must be *Privacy-aware*, *Energy-aware* and *Security-aware* before collaborating. The Quality of Results (QoR) is to be considered to identify acceptable results and make offloading effective [24]. Since the EDCs are capable of limited processing only, a CEC environment helps offloading the processing tasks to other EDCs in the environment. The Fog layer, as shown in Figure 1, helps in scaling the processing but also through load balancing it calls for more secure architecture. The EDCs participating in the load balancing must be verified and authenticated to ensure data security and communication security.

The heterogeneity of the edge computing environment also makes security a challenge and calls for the need to monitor using robust monitoring tools that can provide security against data

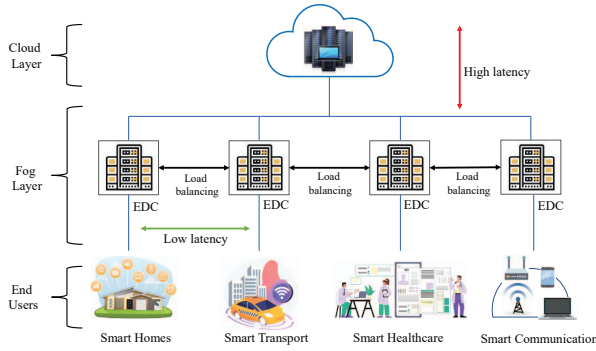


Figure 1: Overview of Edge Data Centers and Load Balancing.

breaches and physical damage to the devices. The technical challenges with respect to security and privacy in smart villages are providing security against device physical damages, DoS (Denial-of-Service) attacks, flooding attacks, forwarding attacks etc. [18]. A Certificate Authority (CA) is a trusted resource that issues Secure Socket Layer (SSL) digital certificates which are a part of the Public Key Infrastructure (PKI). CAs help maintain trust between communicating entities over the internet [14]. The CA helps build a Root-of-Trust between the connected devices in the environment. A centralized CA will be prone to single-point failure whereas a more distributed CA will provide flexible effective security management, and it has scope to generate different cryptographic keys for different authentication processes [11]. This proposed research is a continuation of the research proposed in [1], where XOR Arbiter PUFs are used to develop an authentication system for EDCs in CEC. The paper implements the authentication scheme where EDCs participating in load balancing authenticate each other, along with the edge server acting as an EDC verifying and authenticating authority. The current research is an improvement over the former, in implementing an authentication system where data security and device security is considered.

2 RELATED PRIOR RESEARCH

Covered in this section are the related prior research involving device security and authentication methods. [10] uses PUFs to authenticate IoT devices using the PUF CRPs, in order to minimize the storage space for storing all the CRPs a PUF can generate. It uses only one CRP to store for authentication by message encryption. [23] uses multiple PUFs to authenticate IoT devices in resource constrained environments, and the generated PUFs are not stored or transmitted. The CRP once used during authentication will not be used again, hence reducing the risk of a replay attack and CRP exposure during subsequent authentication. It also reduces the chances of machine learning attacks because of the use of multiple PUFs. An Edge-Assisted Decentralized Authentication Architecture (EADA) is proposed in [21] for vehicular networks. An authentication server is involved, which handles the registration and mutual authentication of the edge nodes. The PUF addresses the fundamental problem of device identification which is essential for Trust

Management. Root-of-Trust can be achieved using PUF-based digital signatures and authentication methods [4]. An Elliptic Curve Encryption (ECC) technology based authentication system is proposed in [20], for security of smart grids. In this method, the device privacy information is encrypted with the use of random numbers and timestamps to increase the security.

A blockchain based privacy preserving authentication protocol for Vehicular Edge Computing (VEC) has been proposed in [22]. It uses smart contracts issued by the certificate authority (CA) to link a public key to the user identity, which can be used for mutual authentication. A secure vault based authentication system to authenticate the IoT devices and IoT server is discussed in [19]. This research uses a multi-key authentication mechanism where the key values keep changing, to overcome the drawbacks of single key authentication systems. A smart contract and blockchain based mutual authentication system for inter-edge and intra-edge devices and servers is presented in [5], which addresses security issues like anonymity and confidentiality in CEC environments. A privacy-aware authentication protocol based on a combination of PUFs and blockchain is proposed in [25], for cloud-edge multi-server IoT systems. In the field of Internet-of-Vehicles (IoV), technologies like blockchain, PUFs, Dynamic Proof-of-Work (dPoW) and consensus algorithms are used to develop a trust management model, where PUFs are used for the unique identity of the vehicle forming the trust element [9]. A comparative summary of these works is given in Table 1.

Table 1: Comparative Table for State-of-the-Art Literature.

Research	Algorithm	Application
Puthal, et al. [17]	AES-based Symmetric Encryption	Authentication and Load Balancing of EDCs
Barbareschi, et al. [3]	PUF based PHEMAP	Fog-IoT Systems
Hathal, et al. [8]	TA, TESLA	Vehicular Communication Systems
Li, et al. [13]	p-KNN	SND-based Edge Computing for Healthcare Systems
Zhang, et al. [25]	SRAM PUF and Blockchain	Multiserver Authentication in Cloud-Edge IoT
Puthal, et al. [15]	Decision Tree	Data aggregation and PoAh for Blockchain in IoT Edge
Aarella, et al. [1]	XORArbiter PUF	Authentication of EDC in CEC
Fortified-Edge (Current Paper)	SRAM PUF based CA	Edge Data Center Authentication in Collaborative Edge Computing

3 CONTRIBUTIONS OF THE CURRENT PAPER

3.1 Problem Addressed

PUFs are hardware security primitives for IoT devices and data centers. PUFs generate CRPs which are stored in the CRP database. These databases are needed for storing the PUF challenges and their responses and the device in question is authenticated based on the verification of the device's response to a given challenge. The CRP database can be stored in the cloud in real-time processing and in CEC scenarios where authentication does not involve the cloud, the CRP database needs to be stored at the edge. Edge infrastructure may not always provide enough storage space and storing database at every EDC is a threat to data security as it can undergo data breach. In CEC where authentication is off cloud, the CRP database needs to be stored at the edge. The size of the database may vary considerably depending on the number of devices involved in the authentication process, and storage space is dependent on the EDC infrastructure. Figure 2 shows the storage space complexity with respect to dynamic load balancing. As the number of nodes to be authenticated increases, the number of CRP sets to be stored also increases. Space is not an issue in static load balancing where one EDC always transfers loads to the same other EDC. In Dynamic load balancing the EDCs can choose any available EDC at that given time among the available EDCs, thus the need for storing more CRP sets for each of the participating EDCs, which in-turn calls for larger storage space. Therefore, we can deploy the security of the PUFs and solve the storage space complexity.

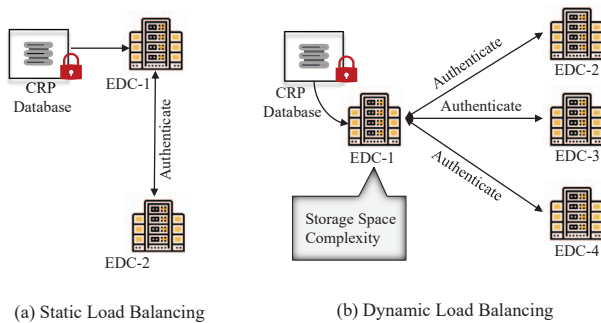


Figure 2: Space Storage Complexity in Dynamic Load Balancing.

In resource constrained environments like the smart villages of the future that head towards CEC, data storage is seen as an issue [16]. Such an environment needs a secure authentication system that does not need more storage space or processing power. Based on these points, the problems that are addressed in this paper are:

- (1) Need for lightweight, secure and robust authentication protocol
- (2) At-the-Edge authentication protocol, without cloud dependency
- (3) A low latency authentication protocol
- (4) Solving the storage space complexity when storing CRP databases that are involved in PUF based authentication schemes
- (5) Data security of the CRP Database

3.2 Solutions Proposed

The PUF CRPs stored in the cloud are highly secure due to the complex cloud security systems and policies. The EDCs at edge rely on mutual authentication like the majority of IoT devices. Mutual authentication is achieved using methods like (i) Symmetric Cryptography Algorithms, (ii) Public Key Infrastructure (PKI) and other mechanisms. In this research we propose the following solutions for PUF based authentication scheme [7]:

- (1) Edge server based architecture for EDC verification and authentication without cloud
- (2) XORArbiter PUF based authentication scheme for EDC verification and authentication, to identify the EDCs by registering them through a client-server authentication protocol
- (3) A mutual authentication scheme for client-client authentication during load balancing
- (4) Removing the need for storing a CRP database locally at the EDC, hence reducing the risk of data compromise
- (5) SRAM PUF based certificate generation to establish root-of-trust between EDCs participating in load balancing
- (6) Mutual authentication scheme based on certificates

3.3 Novelty and Significance of the Proposed Work

The purpose of EDCs in CEC is to perform real-time processing close to the edge and reduce latency. The distributed work handling model of the data centers through load balancing ensures the faster completion of tasks and maximum utilization of available processing times at various data centers. All EDCs will not have the same infrastructure and in environments like smart villages we cannot expect them to provide storage space for complex authentication systems. The aim is to achieve the main security features of IoT edge, like Confidentiality, Integrity, Availability, Identification and Authentication, Privacy and Trust. In the current paper we propose these following approaches for a lightweight, secure, and low latency authentication process for the EDCs:

- (1) CA based authentication to overcome the need for storing CRP database in the EDCs
- (2) Reducing the storage space requirement at EDC, enhancing data security
- (3) PUF as the lightweight, robust and secure mode of key generation
- (4) Using servers at the edge instead of the cloud
- (5) A robust and secure EDC mutual authentication scheme during load balancing using SRAM PUF for certificate generation

4 THE PROPOSED PUF CA METHOD

The proposed scheme mainly focuses on removing the need for storing the CRP database locally in the EDCs, which participate in load balancing and use PUF based security schemes for authenticating each other. Hence, we propose a scheme where a *Verification and Authentication Server* is centrally placed in the *Fog Layer*, making it independent of the cloud server. SRAM PUFs have applications in secure key generation, device authentication, data protection,

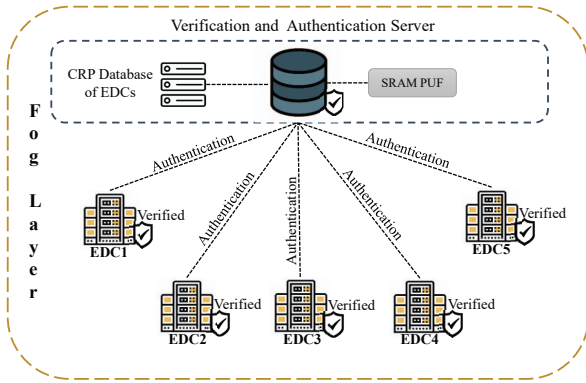


Figure 3: Architecture of the proposed PUF based CA scheme.

chip asset management, anti-counterfeiting, anti-cloning, supply-chain protection ,etc. The architecture of the SRAM PUF based CA scheme is shown in Figure 3.

The PUF keys generated from the given input data and the digital fingerprint of the SRAM PUF are the responses which are stored in the CRP database of the *Verification and Authentication Server*. The generated key code contains a 32-bit key header, which includes the *Key Index*, ranging from 0-15, and *Key Size* which ranges from 64-bits to 4096-bits. The digital fingerprint is generated when the SRAM PUF is powered up, the startup data from the SRAM PUF combined with the Activation code input generates the digital fingerprint of the SRAM PUF. This 256-bit digital fingerprint is the root key used for encryption/decryption of the user keys. The SRAM PUF bits can be extracted with lower error rates using different extractor algorithms and error correction algorithms, through which stable PUF bits can be generated [12].

4.1 Certificate Generation

The PUF based Certificate is generated by Algorithm 1. First the EDCs register themselves with the *Verification and Authentication server* by sending a request including its device ID and MacID. The server verifies the information and sends the PUF challenge from the PUF CRP database. To make the CRP data inaccessible to external communication it is important to avoid any access to the PUF once the device is enrolled [2]. SHA256 is used as the hashing engine. The challenge and response are verified, the EDC is registered, and a Digital Certificate is generated which includes the following information:

- Certificate Version - C_v
- Certificate Serial Number - C_s
- Issuer ID - C_i
- Validity Period with Timestamp - C_d
- Edge Data Center ID - E_i
- Digital Signature - D_s

Algorithm 1: Algorithm for Server Verifying EDC and Sending Certificate.

Input: Recieve EDC certification request with payload

Output: Verify EDC and send Certificate from Authentication Server

```

1 Client request recieved ;
2 get MacID ;
3 if  $MacID_c = MacID_s$  then
4   EDC is Identified;
5 else
6   EDC is NOT Identified ;
7   Registration NOT Successful ;
8 Send random challenge  $C_r$  based on EDC ID ;
9 Get PUF response  $R_p$  ;
10 if  $R_p \neq R_s$  then
11   EDC is NOT Authenticated ;
12   Registration NOT Successful ;
13 else
14   Registration Successful ;
15   Generate Certificate ;
16   Create hashString =  $(C_v, C_s, C_i, C_d, E_i, D_s)$  ;
17   Compute hash (hashString) ;
18   Generate Private Key  $P_k$  ;
19   Create Digital Signature =  $(hashString' + P_k)$  ;
20 Send Digitally signed Certificate to EDC ;
/* The Certificate Authority module will generate the
   authentication certificate and send it to the EDC
   to store. */

```

Algorithm 2: Algorithm for EDCs Mutual Authentication during load Balancing.

Input: Recieve Authentication request from EDC with payload

Output: Authenticate the EDC based on Certificate

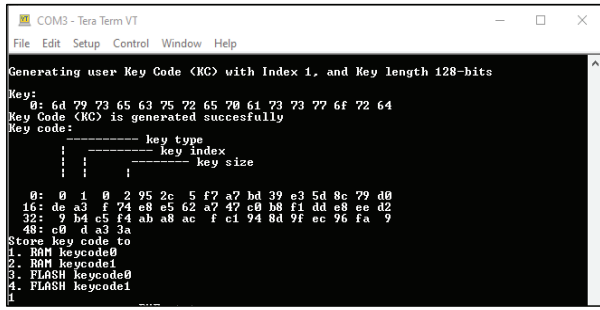
```

1 Authentication request recieved ;
2 Send Certificate ;
3 Get Certificate ;
4 Check validity Period ;
5 if Valid then
6   Get Public Key  $P_u$  ;
7   Verify Digital Signature =  $(hashString' + P_u)$ ;
8 if Verified then
9   Successfully Verified ;
/* The EDCs will exchange the certificates verify the
   validity period and digital signature, if it is
   valid they participate in load balancing */

```

4.2 EDC Mutual Authentication during Load Balancing

During Load balancing the EDCs participating in load balancing must authenticate each other before offloading the tasks. The authentication scheme discussed here uses the Certificates of the EDCs to authenticate each other. The requesting EDC will send an authentication request to the participating EDC which will respond by sending the PUF based certificate encrypted with its private key.



```

COM3 - Tera Term VT
File Edit Setup Control Window Help
Generating user Key Code (KC) with Index 1, and Key length 128-bits
Key:
0: 6d 79 73 65 63 75 72 65 70 61 73 73 77 6f 72 64
Key Code (KC) is generated successfully
Key code:
-----key type
|         key index
|         key size
-----
0: 0 1 0 2 95 2c 5 f7 a7 bd 39 e3 5d 8c 79 d0
16: de a3 f 74 e8 e5 62 a7 47 e9 b8 f1 dd e8 ee d2
32: 9 b4 e5 f4 ab a8 ac f c1 94 8d 9f ec 96 fa 9
48: c0 d a3 3a
Store key code to
1. RAM keycode0
2. RAM keycode1
3. FLASH keycode0
4. FLASH keycode1
1

```

Figure 4: Keycode generated from the SRAM PUF module.

The requesting EDC will decrypt the payload with its public key and verify the validity of the certificate. If the certificate is valid the EDC will authenticate the participating EDC and begins the communication for task offloading, as shown in Algorithm 2.

5 EXPERIMENTAL RESULTS

5.1 Experimental Setup

The Verification and Authentication Server is a Raspberry Pi 4 with Okdo E1 development board used as an SRAM PUF module. MCUXpresso Integrated Development Environment along with LCPXpresso55S69 SDK is used for SRAM PUF key generation. The SRAM PUF module is responsible for generating the Private Key for signing the Digital Certificate. The keycode generated is shown in Figure 4. During the enrollment phase of the PUF module the Activation Code is generated which is used along with the PUF algorithm to generate the PUF key. The CRP database in the server stores the CRPs from the EDC clients, and Raspberry Pi 4 boards are used as the EDC clients. The PUFs used in the clients are XORArbiter PUFs virtually generated from the pypuf module. Python is used for developing certificate generation and mutual authentication algorithms. For experimental purposes the validity period of the certificate was set up as one day after which the certificate will become invalid.

5.2 Validation and Analysis

The XORArbiter PUFs used for EDC client verification are tested for accuracy and uniqueness. Figure 5 shows the validation and analysis components. The accuracy results from training the varying amount of data on different models is shown in Figure 5(1). To train the models we have used 1000 challenge response pairs, with 64-bit challenges and 1-bit response. The ideal prediction accuracy is expected to be 50%. From the results, it is seen that the prediction accuracy is close enough to the ideal values. The Hamming distance of the 256 bit SRAM PUF keys is found to be 64 bits. Randomness of the SRAM PUF keys is calculated as 50.89

Latency results are shown in Figure 5(2) shows the median latency of the server in handling authentication requests in ms. The system is capable of maintaining the latency with increase in number of requests. The results of load testing the server are shown in Figure 5(3). The graph shows the response time of the server for 1000 client requests sent for verification and authentication. Table 2 shows the comparison of the results with state-of-the-art literature.

Table 2: Comparative Table for State-of-the-Art Literature.

Research	Algorithm	Server Authentication Time	Mutual Authentication Time
Barbareschi, et al.[3]	PUF based PHEMAP	NA	38.58ms
Hathal, et al.[8]	TA, TESLA	NA	8600ms
Zhang, et al. [25]	SRAM PUF and Blockchain	3302.9ms	991.8ms
Puthal, et al. [15]	Decision Tree(DT)	NA	0.6s to 0.803s
Aarella, et al. [1]	XORArbiter PUF	0.5s -1.5s	500ms
Fortified-Edge (Current Paper)	PUF based CA	<1500ms	500ms

6 CONCLUSION

PUF based authentication systems are proven to be a secure and lightweight scheme in IoT applications that involves authentication of client devices by servers and authentication of IoT user devices by the clients. From the analysis it is shown that the mutual authentication of EDCs during load balancing takes less than 500 ms, hence reducing the latency. The Fog server-based certificate generation and issuing scheme also reduces the latency involved with a cloud-based server. The use of SRAM PUFs to generate certificates ensures the security of the authentication system. The certificate-based authentication scheme discussed in this research removes the need for storing the CRP database at the client end, making it safe from external attackers accessing the database.

For future research and development of the developed scheme, we propose extensive security analysis against external attacks like man-in-the-middle, spoofing attacks, machine learning attacks etc. Another objective is to design a PUF based Security-by-Design (SbD) model for developing secure IoT applications for Smart Villages.

REFERENCES

- [1] Seema Aarella, Saraju P Mohanty, Elias Kougiianos, and Deepak Puthal. 2022. PUF Based Authentication Scheme for Edge Data Centers in Collaborative Edge Computing. In *2022 IEEE International Symposium on Smart Electronic Systems (iSES) (IEEE-iSES-2022)*. Warangal, India.
- [2] Amir Ali-Pour, David Hely, Vincent Beroulle, and Giorgio Di Natale. 2022. Strong PUF Enrollment with Machine Learning: A Methodical Approach. *Electronics* 11, 4 (2022). <https://doi.org/10.3390/electronics11040653>
- [3] Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino Mazzeo, and Nicola Mazzocca. 2019. PUF-Enabled Authentication-as-a-Service in Fog-IoT Systems. In *IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. 58–63. <https://doi.org/10.1109/WETICE.2019.00020>
- [4] Anupam Chattopadhyay, Kwok-Yan Lam, and Yaswanth Tavva. 2021. Autonomous Vehicle: Security by Design. *IEEE Transactions on Intelligent Transportation Systems* 22, 11 (2021), 7015–7029. <https://doi.org/10.1109/ITITS.2020.3000797>

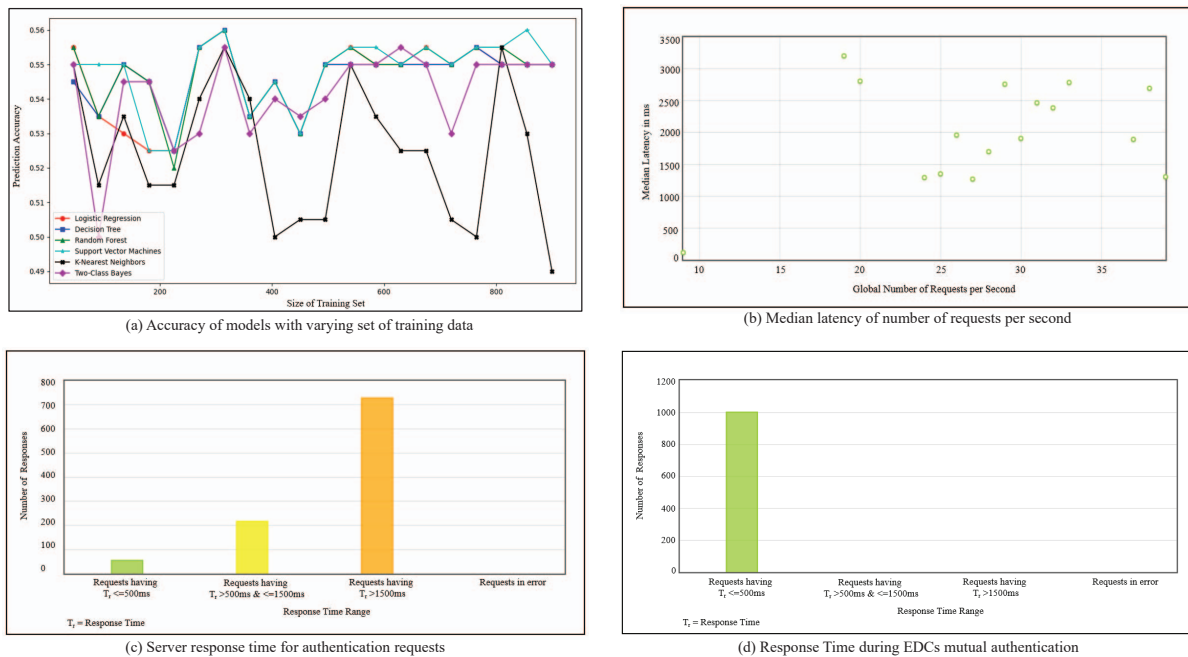


Figure 5: Accuracy of various models, median latency, server response times and mutual authentication time response.

[5] Guanjie Cheng, Yan Chen, Shuiguang Deng, Honghao Gao, and Jianwei Yin. 2022. A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing. *IEEE Transactions on Computational Social Systems* 9, 1 (2022), 146–158. <https://doi.org/10.1109/TCSS.2021.3056540>

[6] Lei Cui, Gang Xie, Youyang Qu, Longxiang Gao, and Yunyun Yang. 2018. Security and Privacy in Smart Cities: Challenges and Opportunities. *IEEE Access* 6 (2018), 46134–46145. <https://doi.org/10.1109/ACCESS.2018.2853985>

[7] Ivan Farris, Tarik Taleb, Yacine Khettab, and Jaeseung Song. 2019. A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems. *IEEE Communications Surveys and Tutorials* 21, 1 (2019), 812–837. <https://doi.org/10.1109/COMST.2018.2862350>

[8] Waleed Hathal, Haitham Cruickshank, Zhili Sun, and Carsten Maple. 2020. Certificateless and Lightweight Authentication Scheme for Vehicular Communication Networks. *IEEE Transactions on Vehicular Technology* 69, 12 (2020), 16110–16125. <https://doi.org/10.1109/TVT.2020.3042431>

[9] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar. 2020. A Scalable Protocol for Driving Trust Management in Internet of Vehicles With Blockchain. *IEEE Internet of Things Journal* 7, 12 (2020), 11815–11829. <https://doi.org/10.1109/JIOT.2020.3002711>

[10] Byoungkoo Kim, Seoungyong Yoon, Yousung Kang, and Dooho Choi. 2019. PUF based IoT Device Authentication Scheme. In *2019 International Conference on Information and Communication Technology Convergence (ICTC)*. 1460–1462. <https://doi.org/10.1109/ICTC46691.2019.8939751>

[11] Hokeun Kim and Edward A. Lee. 2017. Authentication and Authorization for the Internet of Things. *IT Professional* 19, 5 (2017), 27–33. <https://doi.org/10.1109/MITP.2017.3680960>

[12] Ashwija Reddy Korenda, Fatemeh Afghah, Bertrand Cambou, and Christopher Philabaum. 2019. A Proof of Concept SRAM-based Physically Unclonable Function (PUF) Key Generation Mechanism for IoT Devices. In *16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 1–8. <https://doi.org/10.1109/SAHCN.2019.8824887>

[13] Junxia Li, Jinjin Cai, Fazlullah Khan, Ateeq Ur Rehman, Venki Balasubramaniam, Jiangfeng Sun, and P. Venu. 2020. A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System. *IEEE Access* 8 (2020), 135479–135490. <https://doi.org/10.1109/ACCESS.2020.3011503>

[14] R. Perlman. 1999. An overview of PKI trust models. *IEEE Network* 13, 6 (1999), 38–43. <https://doi.org/10.1109/65.806987>

[15] Deepak Puthal, Ernesto Damiani, and Saraju P. Mohanty. 2022. Secure and Scalable Collaborative Edge Computing using Decision Tree. In *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 247–252. <https://doi.org/10.1109/ISVLSI54635.2022.00055>

[16] Deepak Puthal, Saraju P. Mohanty, Stanly Wilson, and Uma Choppali. 2021. Collaborative Edge Computing for Smart Villages [Energy and Security]. *IEEE Consumer Electronics Magazine* 10, 3 (2021), 68–71. <https://doi.org/10.1109/MCE.2021.3051813>

[17] Deepak Puthal, Mohammad S. Obaidat, Priyadarsi Nanda, Mukesh Prasad, Saraju P. Mohanty, and Albert Y. Zomaya. 2018. Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing. *IEEE Communications Magazine* 56, 5 (2018), 60–65. <https://doi.org/10.1109/MCOM.2018.1700795>

[18] Rohani Rohan, Debajyoti Pal, Bunthit Watanapa, and Suree Funilkul. 2022. Emerging Paradigm of IoT Enabled Smart Villages. In *2022 IEEE International Conference on Consumer Electronics (ICCE)*. 1–6. <https://doi.org/10.1109/ICCE53296.2022.9730482>

[19] Trusit Shah and S Venkatesan. 2018. Authentication of IoT Device and IoT Server Using Secure Vaults. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 819–824. <https://doi.org/10.1109/TrustCom/BigDataSE.2018.00117>

[20] Lijun Xiao, Jiahong Cai, Meikang Qiu, and Meiqin Liu. 2021. A Secure Identity Authentication Protocol for Edge Data in Smart Grid Environment. In *8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. 188–193. <https://doi.org/10.1109/CSCloud-EdgeCom52276.2021.00042>

[21] Anjia Yang, Jian Weng, Kan Yang, Cheng Huang, and Xuemin Shen. 2022. Delegating Authentication to Edge: A Decentralized Authentication Architecture for Vehicular Networks. *IEEE Transactions on Intelligent Transportation Systems* 23, 2 (2022), 1284–1298. <https://doi.org/10.1109/ITITS.2020.3024000>

[22] Jianing Yang, Jing Liu, Hengxian Song, Jialu Liu, and Xinyu Lei. 2022. Blockchain-based Conditional Privacy-Preserving Authentication Protocol with Implicit Certificates for Vehicular Edge Computing. In *7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*. 210–216. <https://doi.org/10.1109/ICCCBDA55098.2022.9778897>

[23] Seungyong Yoon, Byoungkoo Kim, and Yousung Kang. 2021. Multiple PUF-based lightweight authentication method in the IoT. In *2021 International Conference on Information and Communication Technology Convergence (ICTC)*. 1198–1200. <https://doi.org/10.1109/ICTC52510.2021.9620972>

[24] Ashkan Yousefpour, Caleb Fung, Tam Nguyen, Krishna Kadiyala, Fatemeh Jalali, Amirreza Niakanlahiji, Jian Kong, and Jason P. Jue. 2019. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* 98 (2019), 289–330. <https://doi.org/10.1016/j.sysarc.2019.02.009>

[25] Yan Zhang, Bing Li, Bo Liu, Yuanyuan Hu, and Haipeng Zheng. 2021. A Privacy-Aware PUFs-Based Multiserver Authentication Protocol in Cloud-Edge IoT Systems Using Blockchain. *IEEE Internet of Things Journal* 8, 18 (2021), 13958–13974. <https://doi.org/10.1109/JIOT.2021.3068410>