PUF-based Authentication Scheme for Edge Data Centers in Collaborative Edge Computing

Presenter: Seema G. Aarella

Seema G. Aarella[1], Saraju P.Mohanty[2], Elias Kougianos[3] , Deepak Puthal[4]

University of North Texas, Denton, TX 76203, USA.[1,2,3]
Khalifa University, Abu Dhabi, UAE.[4]

Email: Seema.Aarella@unt.edu[1], Saraju.Mohanty@unt.edu[2] and Elias.Kougianos@unt.edu[3], deepak.puthal@ku.ac.ae[4]

Outline of the Talk

- Introduction
- Collaborative Edge Computing
- Edge Data Center Authentication
- Related Prior Research
- Novel Contributions of Current Research
- Problems Addressed & Proposed Solutions
- Proposed PUF based Scheme
- Implementation & Results
- Conclusion
- Future Research

Smart Cities Vs Smart Villages

City - An inhabited place of greater size, population, or importance than a town or village

-- Merriam-Webster

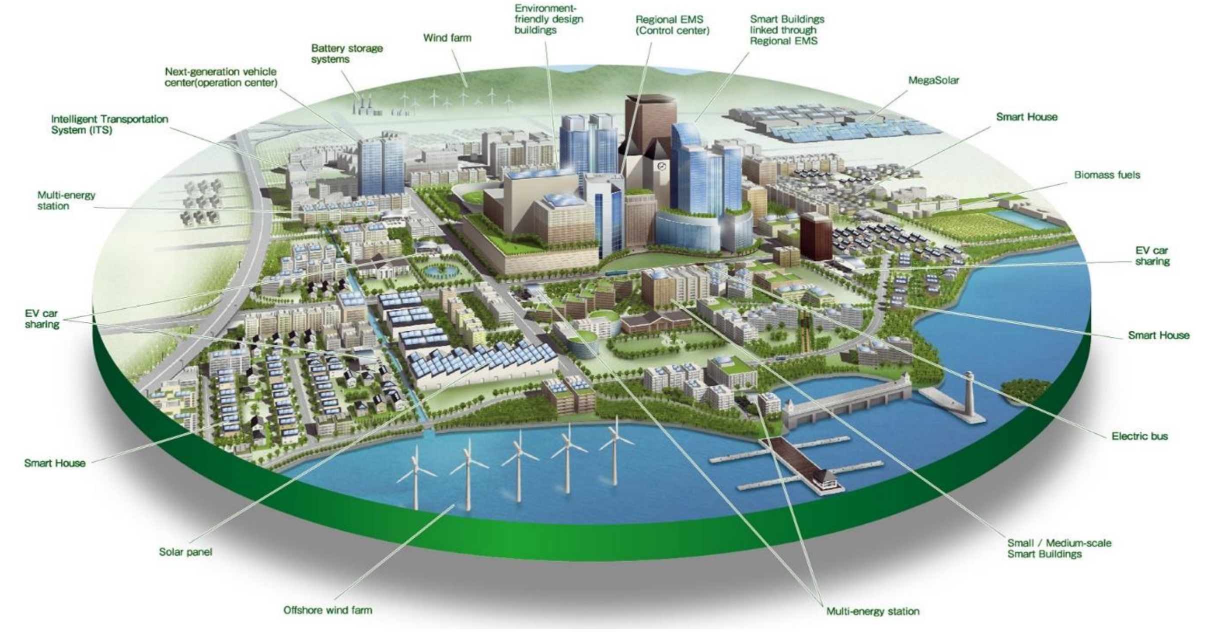
Smart City: A city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city".

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

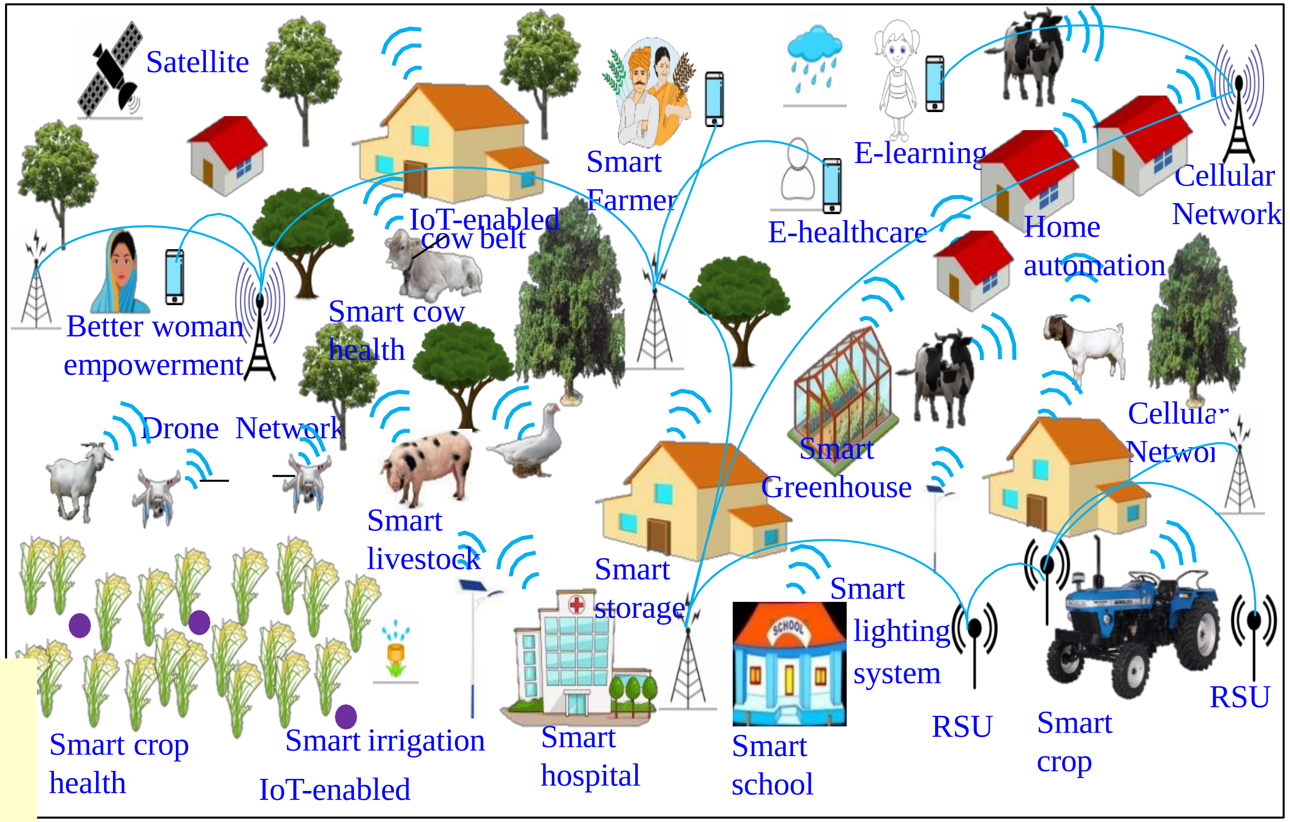
Smart Village: A village that uses information and communication technologies (ICT) for advancing economic and social development to make villages sustainable.

Source: S. K. Ram, B. B. Das, K. K. Mahapatra, S. P. Mohanty, and U. Choppali, "Energy Perspectives in IoT Driven Smart Villages and Smart Cities", *IEEE Consumer Electronics Magazine (MCE)*, Vol. XX, No. YY, ZZ 2021, DOI: 10.1109/MCE.2020.3023293.

Smart Cities Vs Smart Villages



Source: http://edwingarcia.info/2014/04/26/principal/



Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

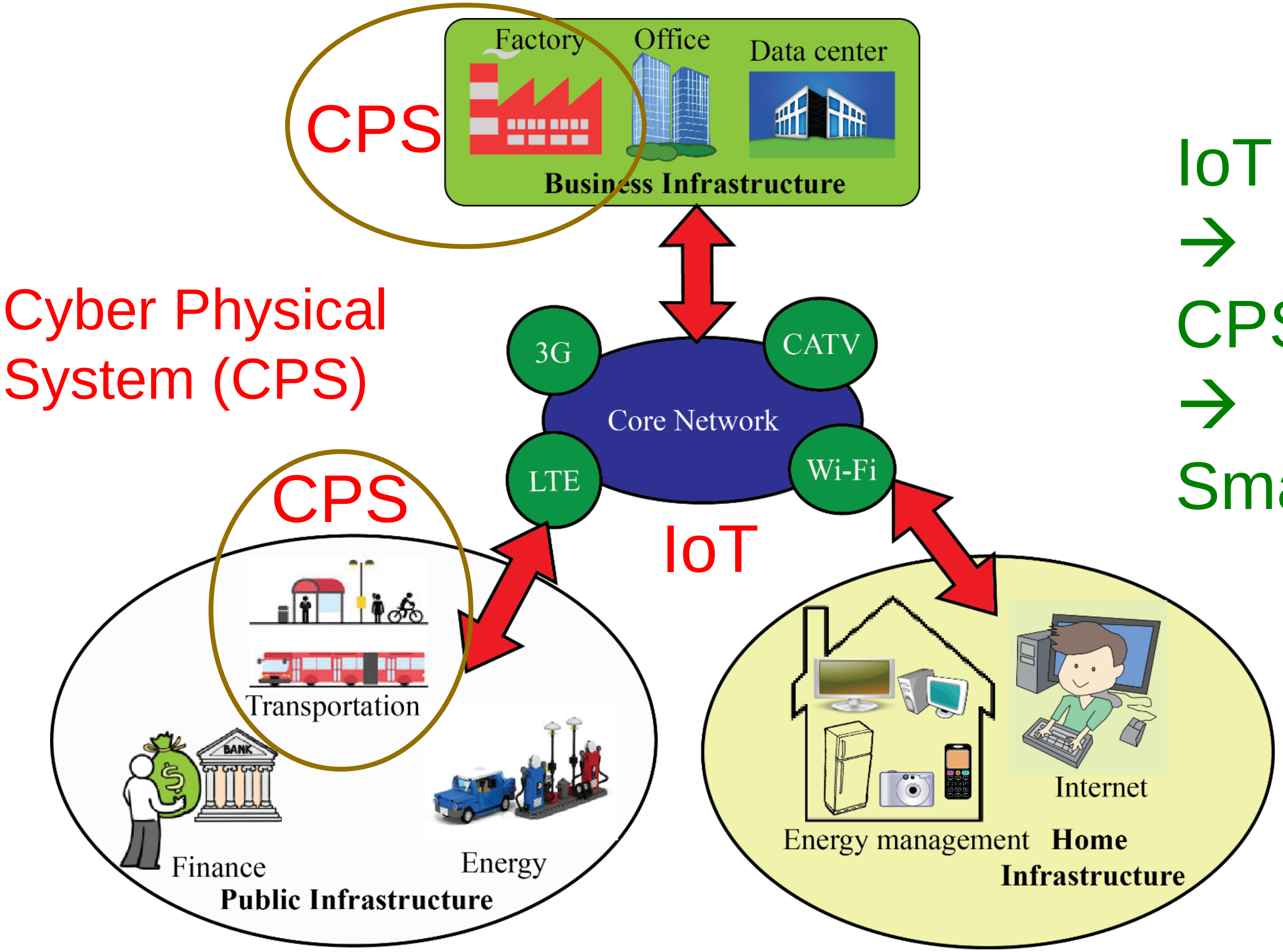
Smart Villages

CPS Types - Less
Design Cost - Low
Operation Cost – Low
Energy Requirement - Low

Smart Cities

CPS Types - More
Design Cost - High
Operation Cost – High
Energy Requirement - High

IoT → CPS → Smart Cities or Smart Villages



IoT
→
CPS (Smart Components)
→
Smart Cities or Smart Villages

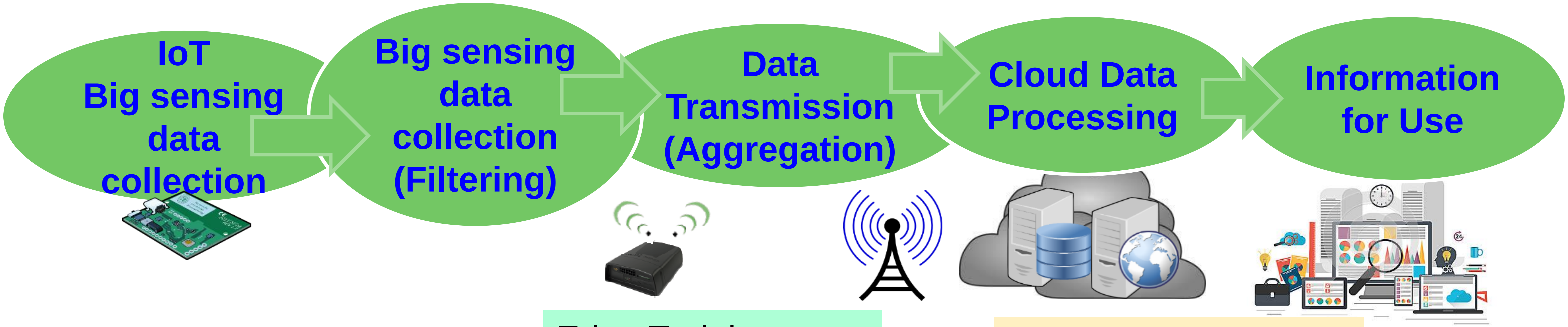
IoT is the backbone

Source: S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Vol. 5, No. 3, July 2016, pp. 60--70.

Bigdata Processing for AI

Source: https://matmatch.com/blog/the-age-of-artificial-intelligence-in-materials-science-part-one/

Data Quality Assurance and Secure Computing in IoT/CPS



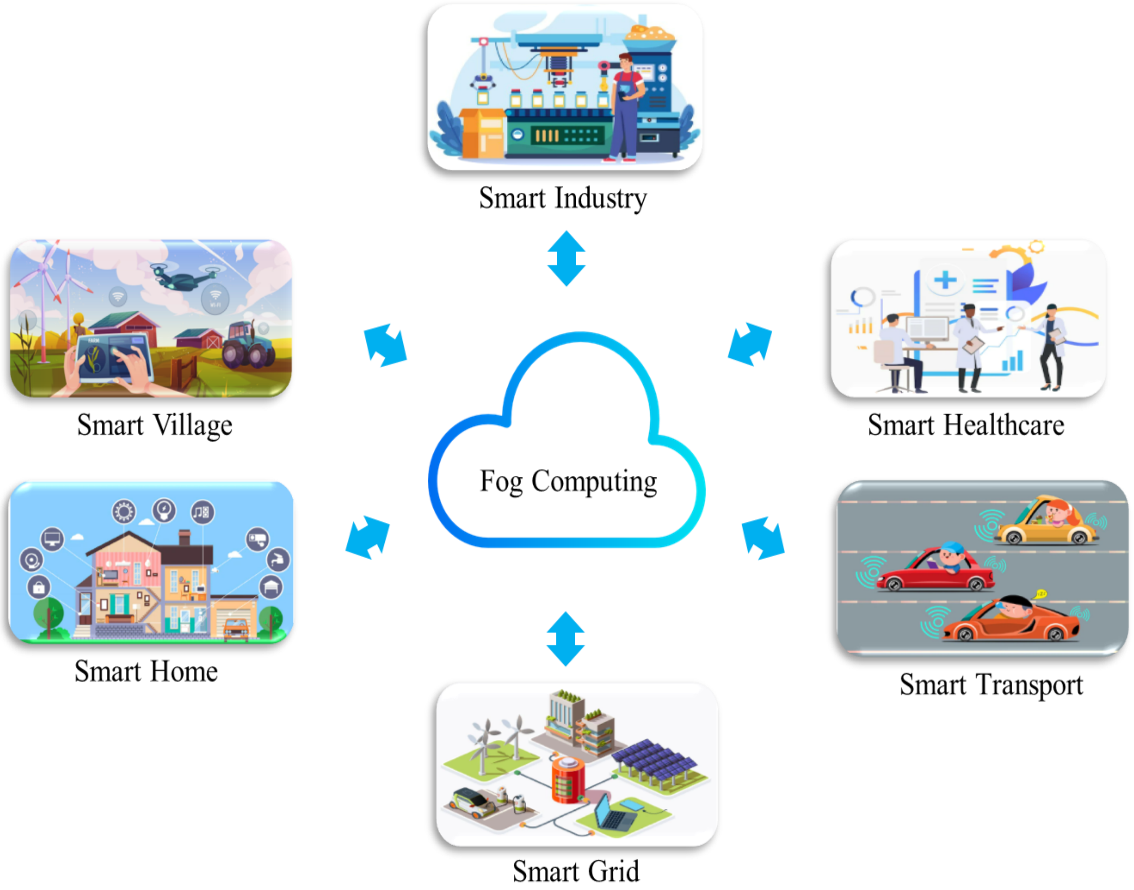
Edge Training:
- Data Signature
- Model Signature

Cloud Training:
- Data Signature
- Model Signature

Source: C. Yang, D. Puthal, S. P. Mohanty, and E. Kougianos, “Big-Sensing-Data Curation for the Cloud is Coming”, *IEEE Consumer Electronics Magazine (CEM)*, Volume 6, Issue 4, October 2017, pp. 48--56.

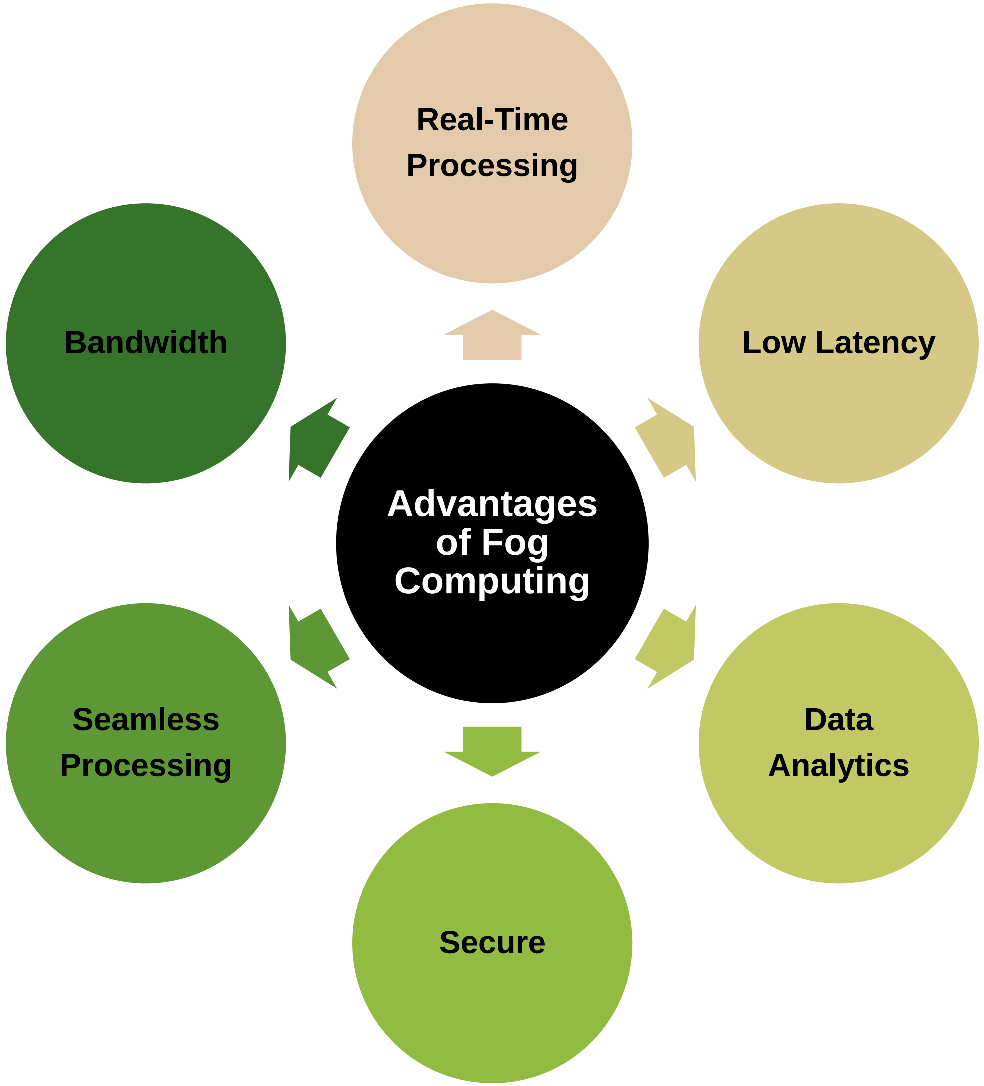
IoT-Cloud Versus IoT-Edge

- Decentralized computing infrastructure lead to Fog and Edge Computing
- Cloud based Authentication schemes have high latency
- Distributed computing requires secure and lightweight authentication systems due to technological limitations in certain environments like smart villages
- Low latency authentication is important in real-time applications like autonomous vehicles
- Resource sharing helps in optimal use of computing power



Fog Computing

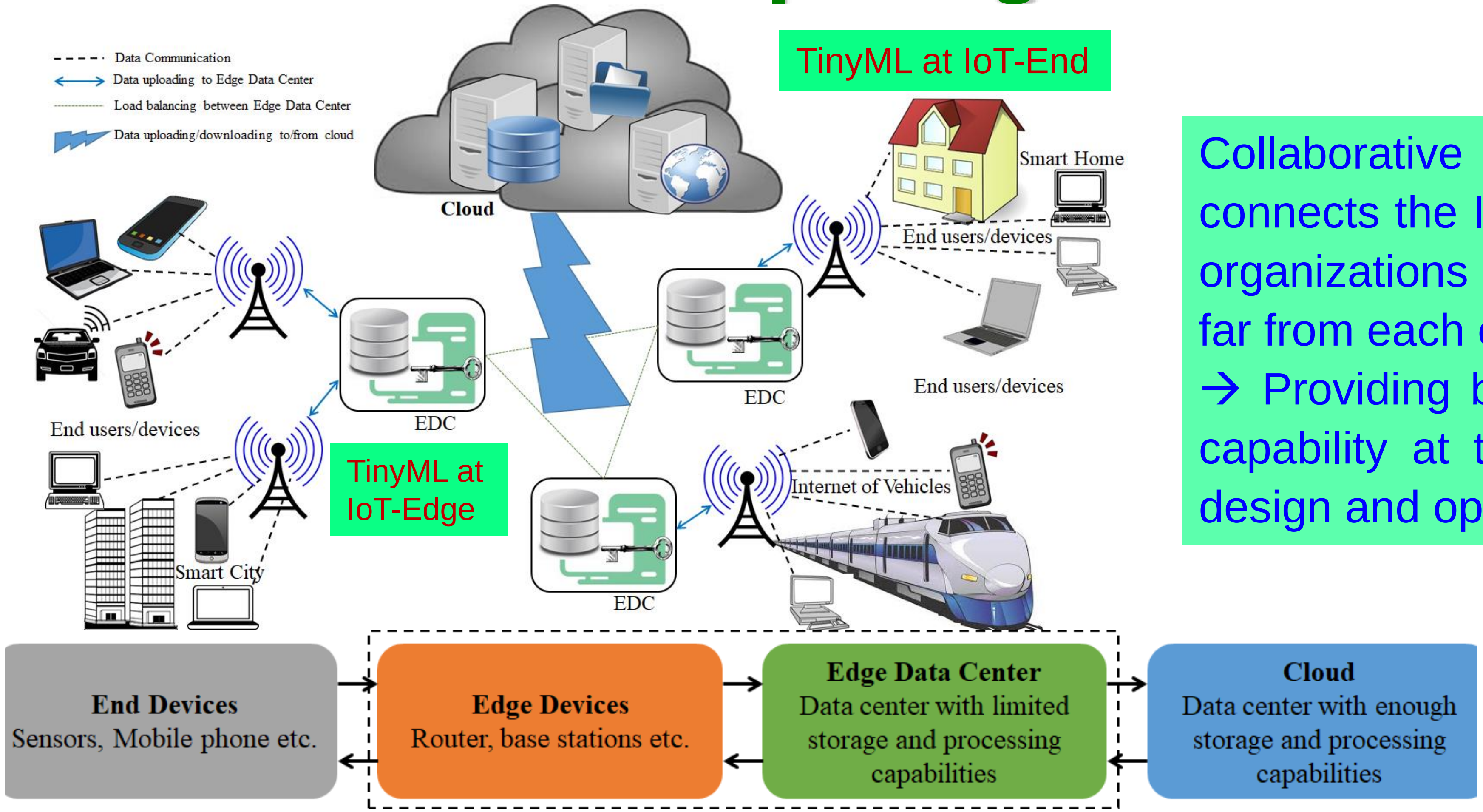
- Fog Computing is a feature of decentralized computing infrastructure
- Fog has nodes between cloud and edge devices
- Fog brings cloud resources closer to edge
- Fog computing involves many Edge Data Centers (EDC)
- EDCs are small data centers located close to edge of a network
- EDCs deliver cloud computing resources to the devices



Our Long-Term Vision

- How to facilitate AI/ML modeling in smart villages where the computing resources are limited?

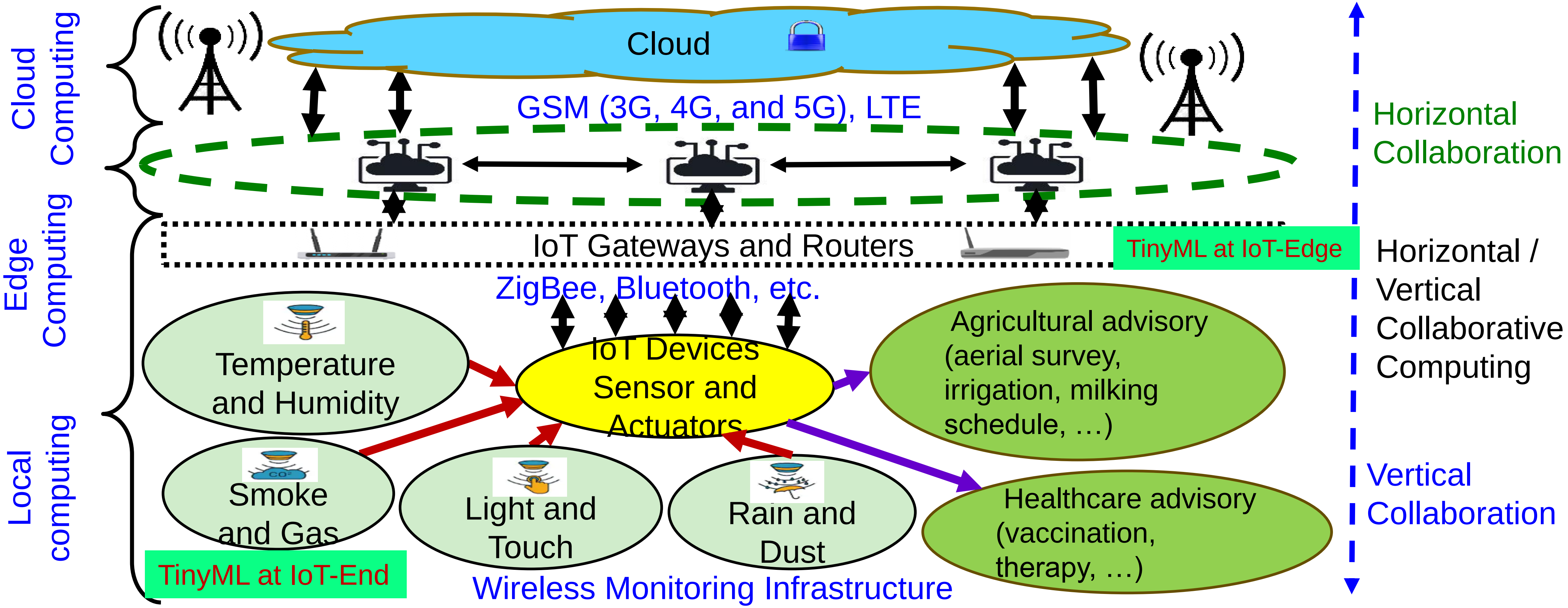
Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



Collaborative edge computing connects the IoT-edges of multiple organizations that can be near or far from each other
→ Providing bigger computational capability at the edge with lower design and operation cost.

Source: D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing”, *IEEE Communications Mag*, Vol. 56, No 5, May 2018, pp. 60--65.

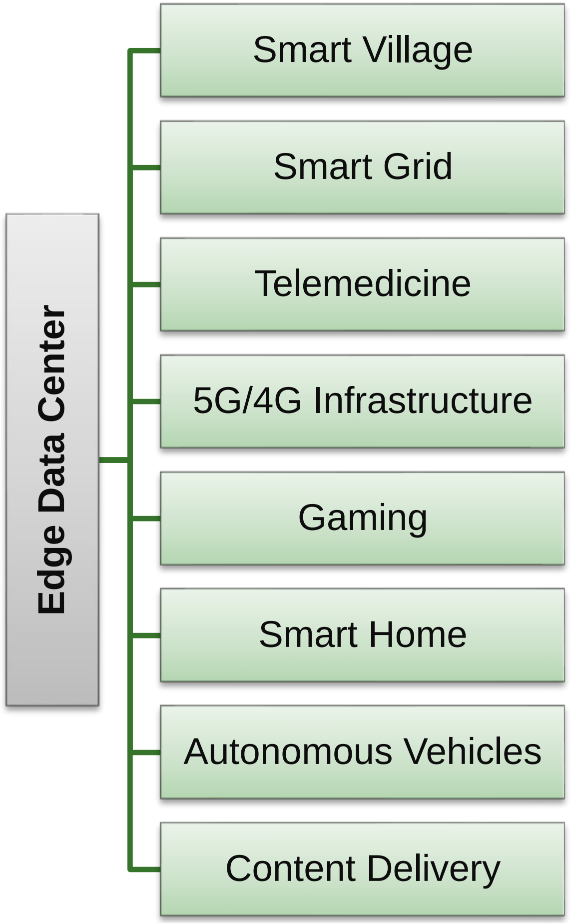
Collaborative Edge Computing is Cost Effective Sustainable Computing for Smart Villages



Source: D. Puthal, S. P. Mohanty, S. Wilson and U. Choppali, “Collaborative Edge Computing for Smart Villages”, *IEEE Consumer Electronics Magazine (MCE)*, Vol. 10, No. 03, May 2021, pp. 68-71.

Collaborative Edge Computing (CEC)

- Collaborative Edge Computing is a distributed processing environment
- CEC is a collaboration of distributed edge
- Smart control of heterogenous network
- Reduced Bandwidth and Transmission costs
- CEC enables seamless processing through load balancing

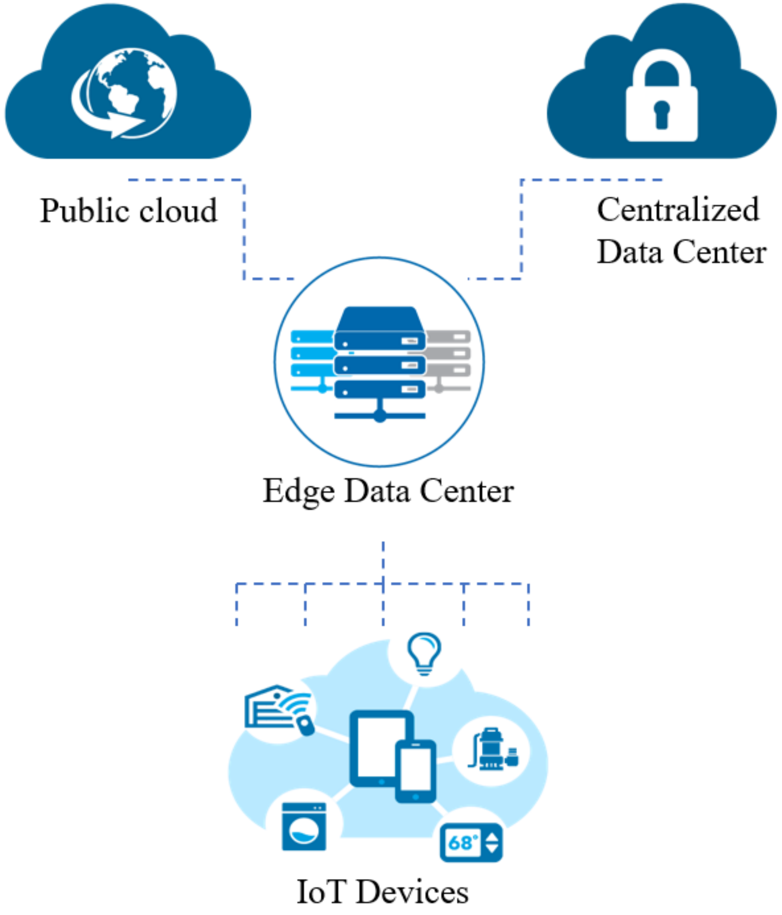


Load Balancing in CEC

- Collaborative Edge Computing helps in overcoming the Technological limitations of certain IoT environments, for ex. Smart Villages
- Limitations like computational resources, continuous & highspeed connectivity, energy for processing, infrastructure and investment
- In distributed computing the Edge Data Centers can offload tasks in a process called load balancing
- Load balancing improves resource utilization and response times
- Static and Dynamic Load balancing can be employed
  - Static Load Balancing – EDC transfers load to same EDC every time
  - Dynamic Load Balancing- EDC transfers task to any other Available EDC in network

Edge Data Center (EDC) in CEC

- Secure authentication for Load balancing
- Edge Data Centers participate in Load Balancing
- EDCs are deployed at different geographical locations
- Lightweight and secure authentication for EDCs
- Cloud Based Authentication causes latency issues
- Risk of Single-point-of-failure



Related Prior Research

Research	Algorithm	Application
Puthal et al. [2022] [1]	Decision Tree (DT)	Data aggregation and Proof-of-Authentication (PoAh) for Blockchain in IoT Edge
Puthal et al. [2018] [2]	AES-based Symmetric Encryption	Authentication and Load Balancing of EDCs
Long et al. [2019] [3]	Double PUF Authentication	IP protection in FPGA trade
Yoon et al. [2021] [4]	Multiple PUF Authentication	IoT device security
Ha et al. [2016] [5]	Elliptic curve cryptography based ECQV	Mutual authentication and key establishment between two resource constrained IoT devices
[Zhang et al. [2021] [6]	PUF based Multi-Server Authentication	PUF based Multi-Server Authentication & Cloud-Edge IoT using Blockchain
Current paper	XORArbiter PUF	Edge Data Center Authentication in Load Balancing

Novel Contributions of Current Research

Virtual XORArbiter PUF implementation and generation

Verification of Edge Data Centers

Using Virtual PUFs to authenticate EDCs

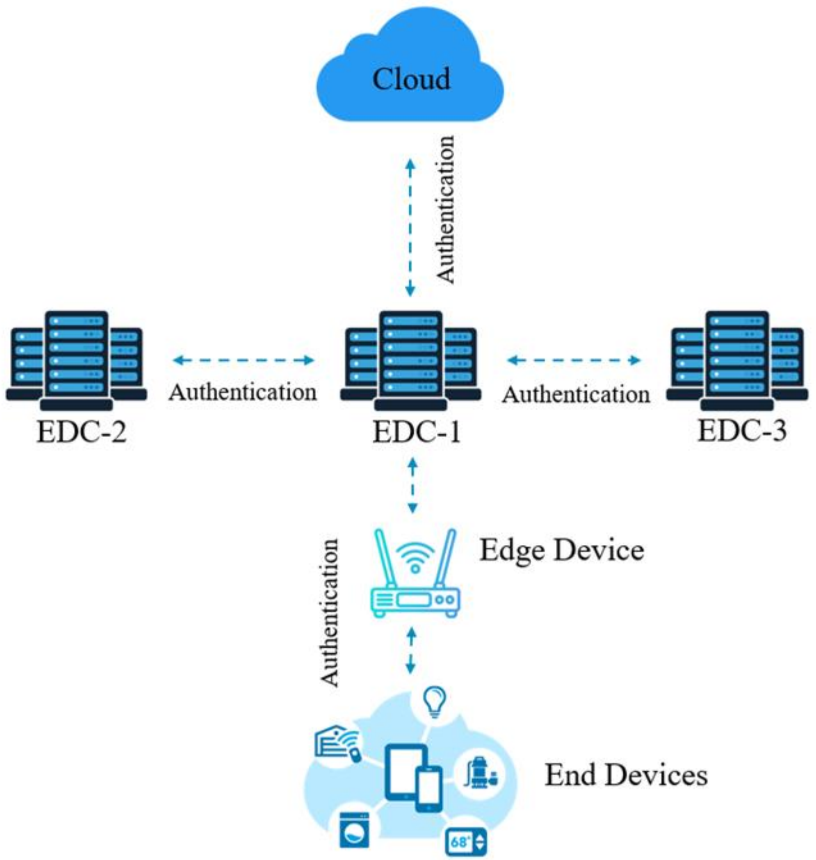
Mutual authentication of EDCs during load balancing without cloud server

Problems Addressed

- Need for robust, secure and lightweight authentication scheme with low computational power
- Authentication without Cloud Server to address latency issues
- Lightweight and Low latency protocol for mutual authentication of EDCs
- Faster and Secure Protocols for authentication

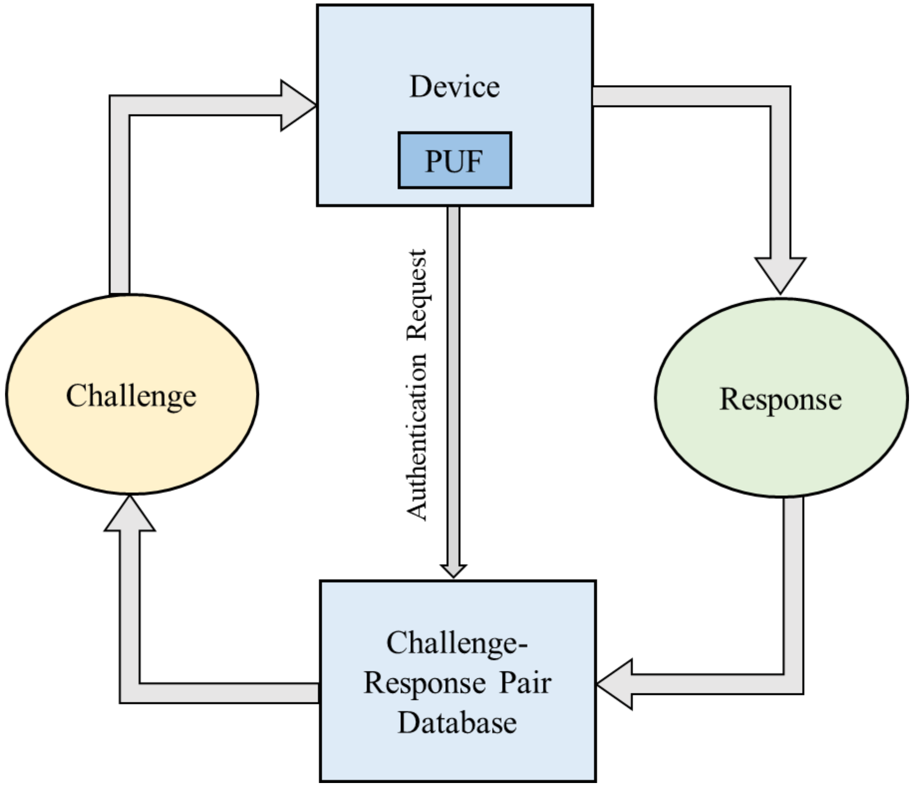
Proposed Solutions

- A PUF-based authentication scheme for Load Balancing
- Virtual XORArbiter PUFs to authenticate the EDCs
- A Mutual Authentication scheme for the EDCs during load balancing
- XORArbiter PUFs to authenticate the user devices connected in the fog environment



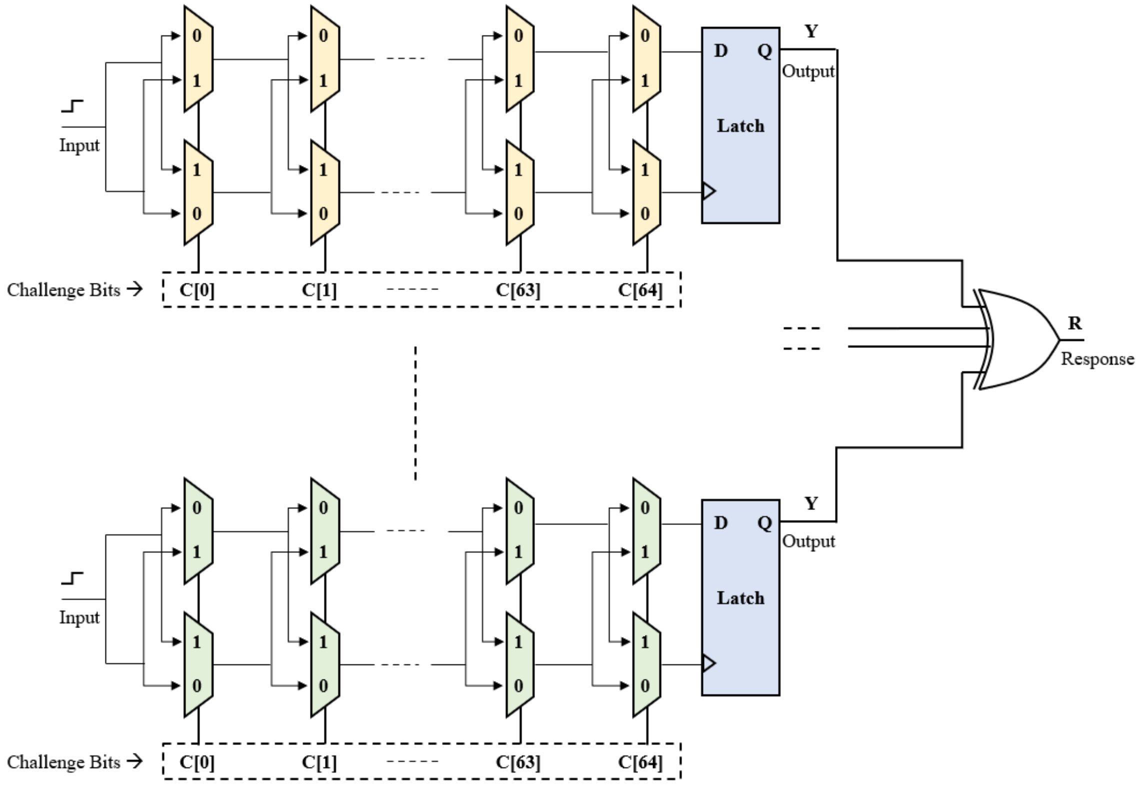
PUF for Authentication

- **Physical Unclonable Functions (PUFs)** use the device's physical variations from which unique keys can be extracted
- **In general, a PUF is used in two steps:**
  - **Enrollment** - Where a number of CRPs (Challenge Response Pairs) are generated from a PUF and stored
  - **Verification or Authentication** – Where device is authenticated based on response to particular challenge
- **Advantages:** Robust, Unique, Unclonable, Less Computational power, No need to store secure keys



Proposed PUF Architecture

- The Arbiter PUF is classified as a delay-based PUF
- The response is generated based on the timing difference in two functionally identical paths in an IC
- An XORArbiter PUF has multiple bit input *C*[*i*] and based on the delay a one bit output *Y* is generated
- The output of an Arbiter PUF is 1 bit
- The arbiter, which is a latch or flip-flop determines the fastest signal
- The arbiter outputs ‘1’ if the upper path is faster; otherwise it will output a ‘0’
- An N-stage arbiter PUF can generate 2N Challenge Response Pairs (CRPs)



Verification and Authentication Scheme

EDC Authentication by Cloud

- The EDC in CEC is verified and authenticated by cloud
- Authentication is done based on PUF challenge-Response
- EDC sends authentication request to server
- Server verifies the digital signature
- Sends challenge to client EDC, and verifies the response in Database
- If the CRPs match the EDC is authenticated

EDC-1 Authenticating EDC-2 without Cloud

- EDC authenticate each other without cloud to reduce latency
- EDC-1 sends a request to EDC-2, which will respond back with the payload encrypted with EDC-2's Pu(Public Key)
- EDC-1 decrypts the payload with its Pr(Private Key), once the EDC-2 is verified
- It sends the 64 bit PUF Challenge, C1, and receives the Response R2 from EDC-2
- If the response matches with the response in the Database the EDC-2 is authenticated and data transfer is initiated

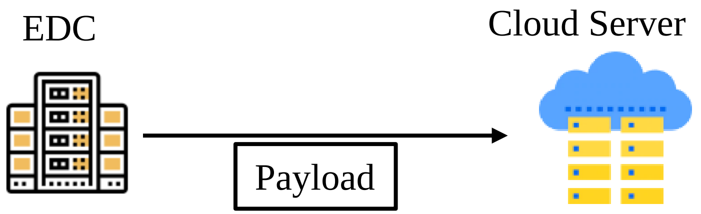
Algorithm-1: EDC Authentication Request

Algorithm 1: Algorithm for EDC sending Authentication Request to Server

Input : EDC (Client) Create Request String, Compute Hash, Create Digital Signature

Output: Send request payload to Server

1. Create authentication request string ;
2. Select random Challenge-Response Pair ;
3. Compute Hash ;
4. Create Private Key ;
5. Generate Digital Signature using the Hash and Private Key ;
6. Append the Digital signature to random CRP and create payload ;
7. Send request to the server ;



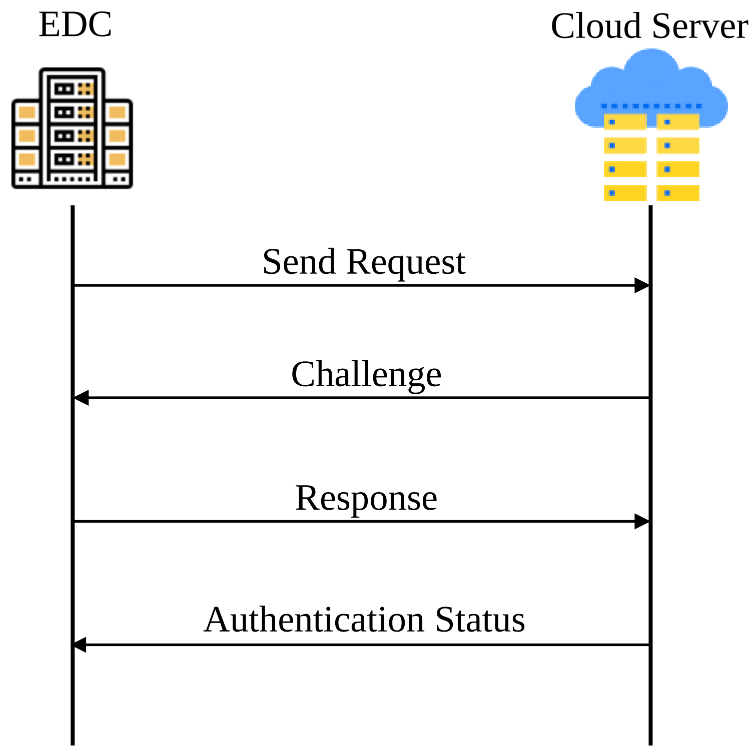
Algorithm-2: EDC Authentication Scheme

Algorithm 2: Algorithm for Server Authenticating the EDC

Input : Receive Client Request with Payload

Output: Verify and Authenticate Client EDC

1. Client request received ;
2. Get MacID;
3. if { MacIDc = MacIDs } then { EDC is Identified};
4. Else { EDC is NOT Identified};
5. Close Connection ;
6. Get Digital Signature ;
7. Verify Digital Signature ;
8. Get PUF Response based on Challenge and EDCID;
9. Verify Response ;
10. if Rc = Rs then {EDC is Authenticated };
11. Else { EDC is NOT Authenticated };
12. Close Connection ;



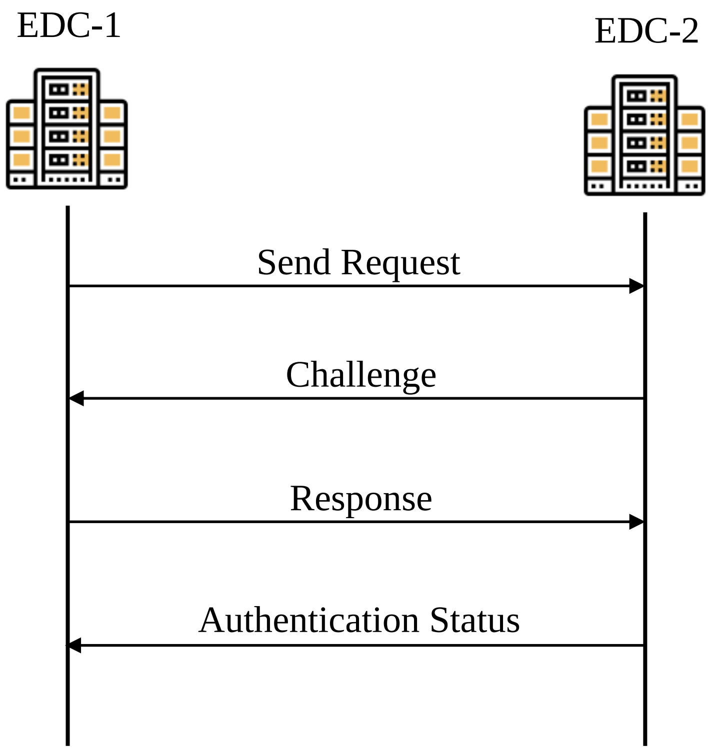
Algorithm-3: Mutual Authentication

Algorithm 3: Algorithm for EDC-1 authenticating EDC-2

Input : Receive EDC-2 Request with Payload

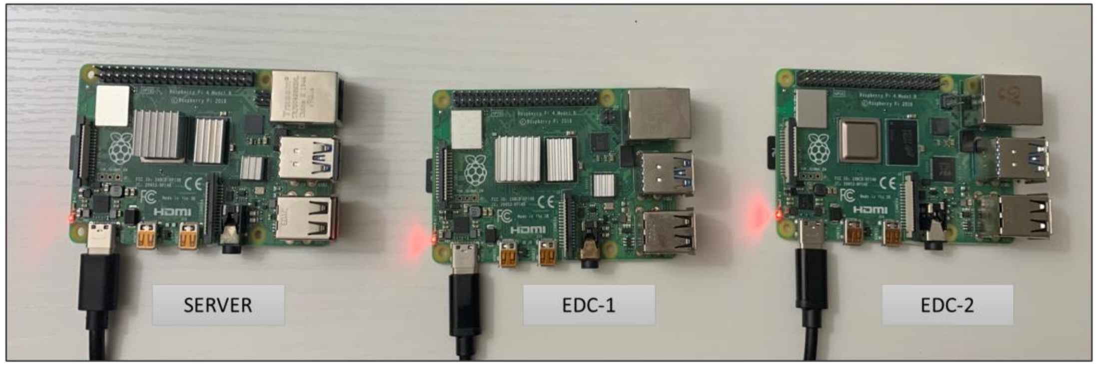
Output: Verify and Authenticate EDC-2

1. EDC-2 request received ;
2. Get MacID;
3. if MacID2 = MacID1 then { EDC-2 is Identified };
4. else { EDC-2 is NOT Identified } ;
5. Close Connection ;
6. Get Digital Signature ;
7. Verify Digital Signature ;
8. Get PUF Response based on Challenge and EDCID ;
9. Verify Response ;
10. if R2 = R1 then { EDC-2 is Authenticated };
11. Close Connection ;
12. else {EDC-2 is NOT Authenticated };



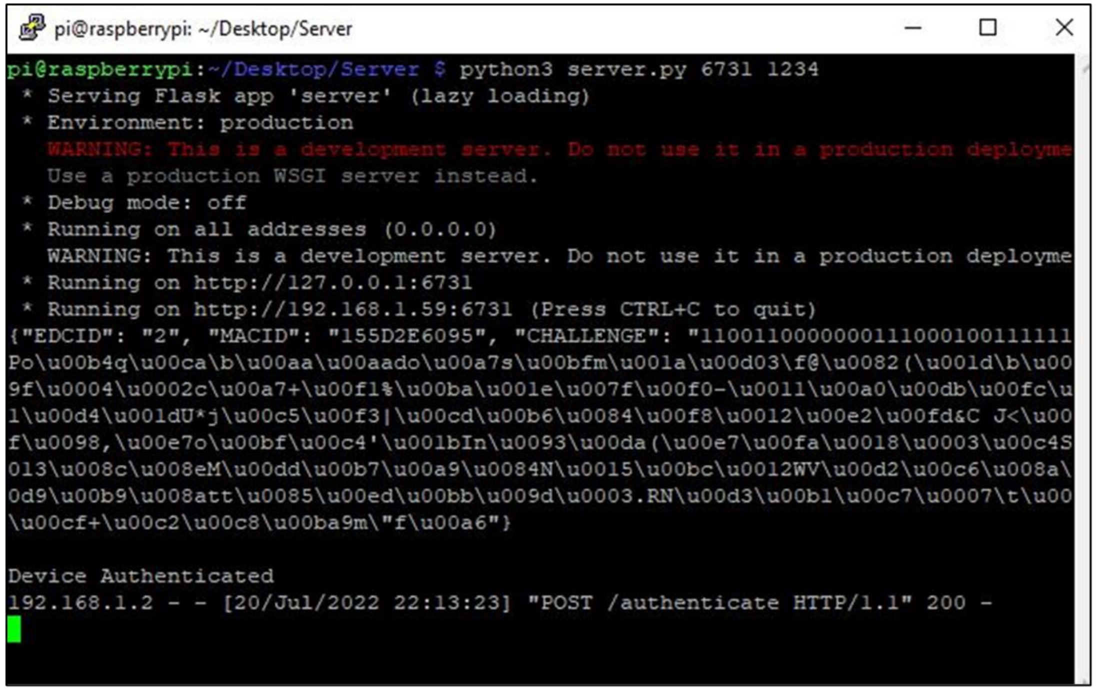
Implementation & Results

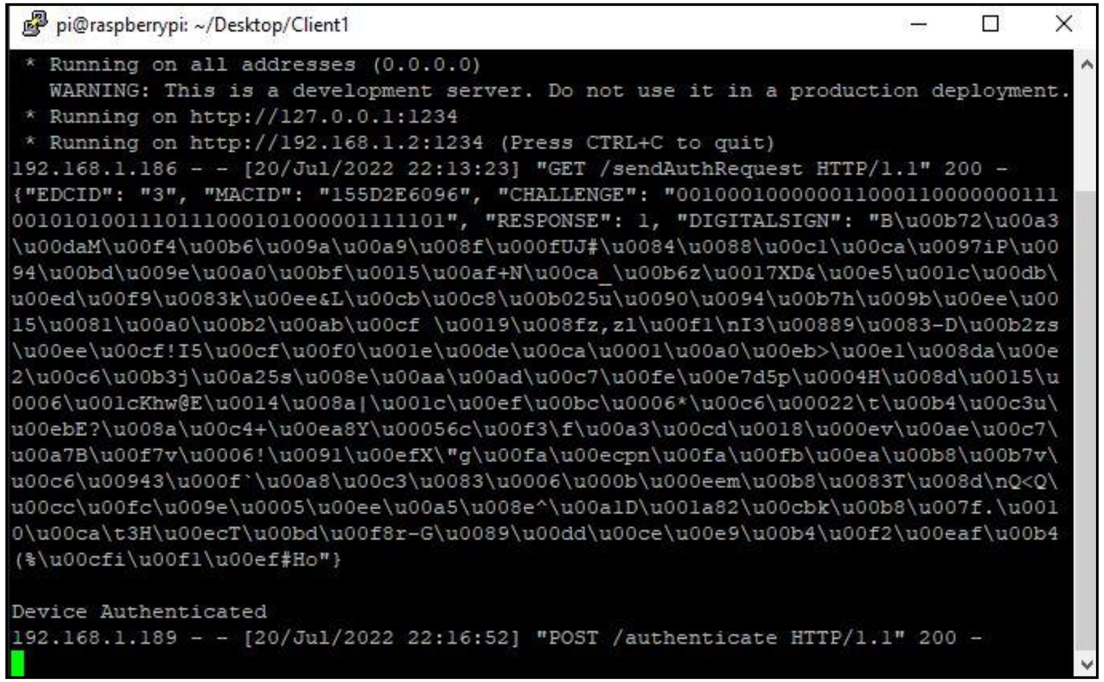
- The EDC authentication scheme is implemented using three Raspberry Pi4 boards, each set up as Server, Client1 (EDC-1) and Client2 (EDC-2)
- The PUF challenge Response Pairs generated from the pypuf package are stored in an SQLite3 database
- The CRPs are unique for each EDC, identified by EDCID
- The challenges are 64-bit and the responses are 1-bit
- SHA256 is used to generate cryptographic hash functions
- The database is considered as the CRP cluster, which serves the EDCs participating in the load balancing



Experimental Results

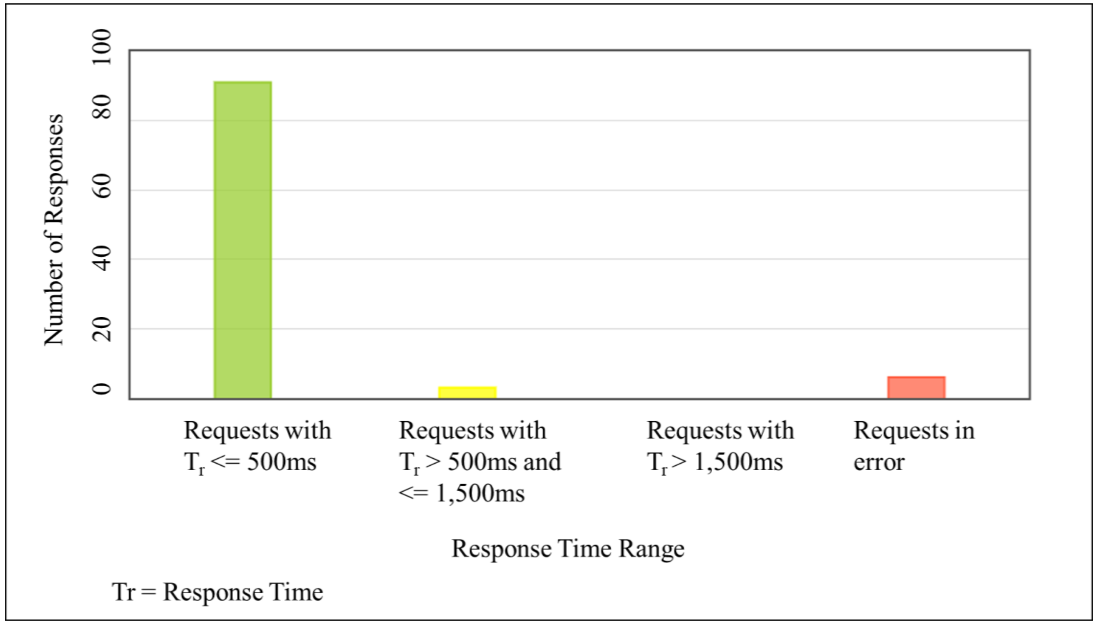
Images of successful device authentication after payload verification

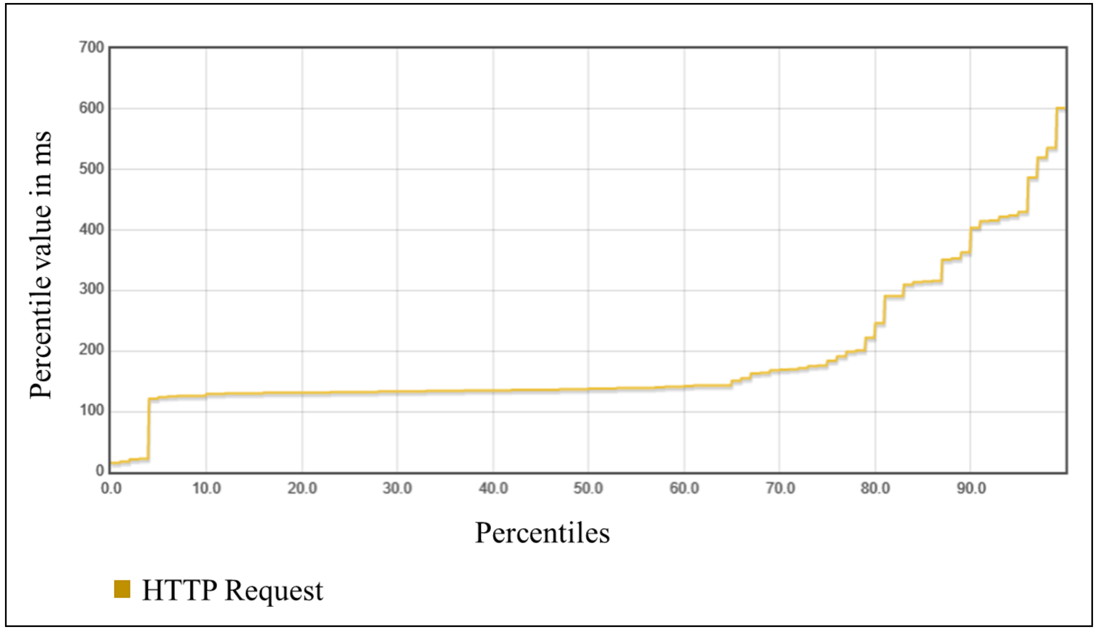




Experimental Results

Load test result of server response to 100 authentication requests





Comparative Analysis

Research	Algorithm	Hamming Distance	Randomness	Authentication Time
Puthal et al. [2022] [1]	Decision Tree(DT)	NA	NA	0.6s to 0.803s
Puthal et al. [2018] [2]	AES-based Symmetric Encryption	NA	NA	NA
Long et al.[2019] [3]	Double PUF Authentication	46.84%	48.64%	NA
Zhang et al. [2021] [6]	PUF based Multi-Server Authentication	NA	NA	3302.9 ms
Current Paper	XOR Arbiter PUF	44.86%	48.47%	< 1500 ms

Conclusion

- Latency and bandwidth are the main concerns when an authentication scheme involves the cloud
- The proposed PUF based EDC authentication scheme proves to be lightweight, highly secure and with low latency, as the cloud is not involved for an EDC authenticating another EDC using the CRP clusters
- An XORArbiter PUF is a strong PUF that adds more non-linearity to the response, thus making it safe against Machine Learning attacks and Power-side channel attacks
- From the results it is seen that the authentication is faster, and the server can handle multiple requests and process them withing 0.5s

Future Research

- We intend to present comprehensive integrated cybersecurity framework for collaborative edge computing in the context of smart villages
- Security Analysis against external attacks
- Motivation: The need for minimal overhead and energy efficient cybersecurity solution for smart village applications under the Security-by-Design(SbD) primitive

References

[1] D. Puthal, E. Damiani and S. P. Mohanty, "Secure and Scalable Collaborative Edge Computing using Decision Tree," 2022 *IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* pp. 247-252.

[2] D. Puthal, M. Obaidat, P. Nanda, M. Prasad, S. Mohanty, and A. Zomaya, “Secure and Sustainable Load Balancing of Edge Data Centers in Fog Computing,” *IEEE Communications Magazine*, vol. 56, pp. 60–65, 05, 2018.

[3] J. Long, W. Liang, K.-C. Li, D. Zhang, M. Tang, and H. Luo, “PUF Based Anonymous Authentication Scheme for Hardware Devices and IPs in Edge Computing Environment,” *IEEE Access,* vol. 7, pp. 124 785–124 796, 2019.

[4] S. Yoon, B. Kim, and Y. Kang, “Multiple PUF-based lightweight authentication method in the IoT,” in Proc. *International Conference on Information and Communication Technology Convergence (ICTC),* 2021, pp. 1198–1200.

[5] D. A. Ha, K. T. Nguyen, and J. K. Zao, “Efficient Authentication of Resource-Constrained IoT Devices Based on ECQV Implicit Certificates and Datagram Transport Layer Security Protocol,” in Proc. *Seventh Symposium on Information and Communication Technology,* 2016, p.173–179.

[6] Y. Zhang, B. Li, B. Liu, Y. Hu, and H. Zheng, “A Privacy-Aware PUFs-Based Multiserver Authentication Protocol in Cloud-Edge IoT Systems Using Blockchain*,” IEEE Internet of Things Journal*, vol. 8, no. 18, pp.13 958–13 974, 2021.

Thank you!