Fortified-Edge 2.0: Machine Learning based Monitoring and Authentication of PUF-Integrated Secure Edge Data Center

Presenter: Seema G. Aarella

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

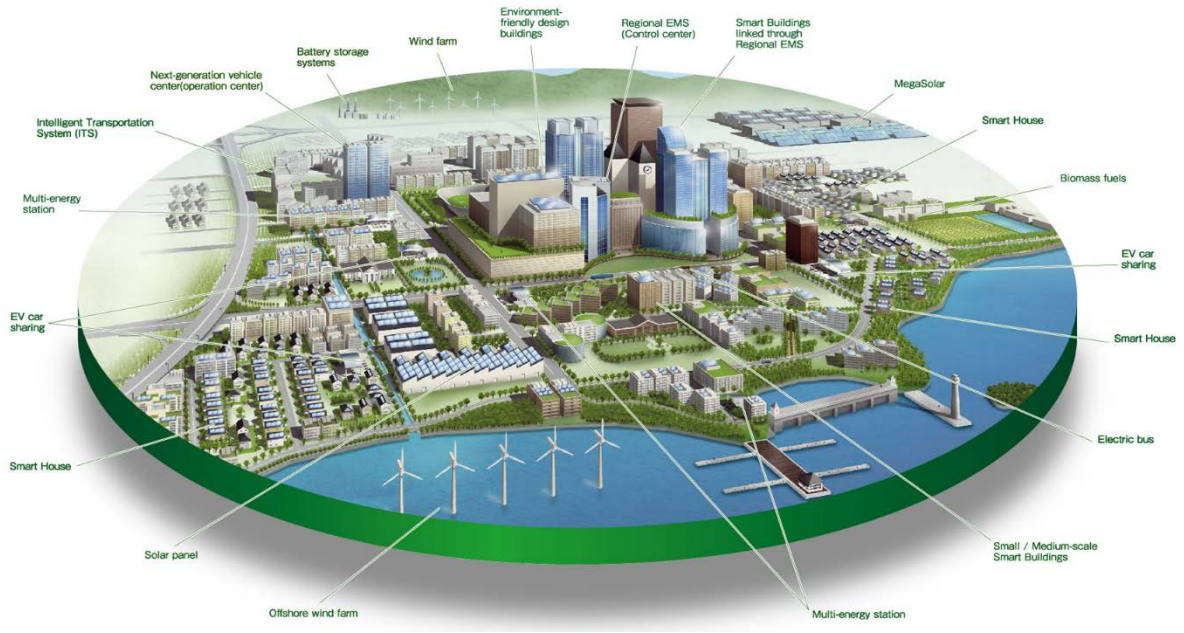
University of North Texas, Denton, TX 76203, USA.[1,2,3]
Khalifa University, Abu Dhabi, UAE.[4]

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
- Smart Cities and Smart Villages
- Need for Security-by-Design
- Collaborative Edge Computing for Smart Village
- ML based Authentication and Monitoring
- Proposed Fortified-Edge 2.0
- Experimental Results
- Conclusion
- Future Research

Smart Cities Vs Smart Villages



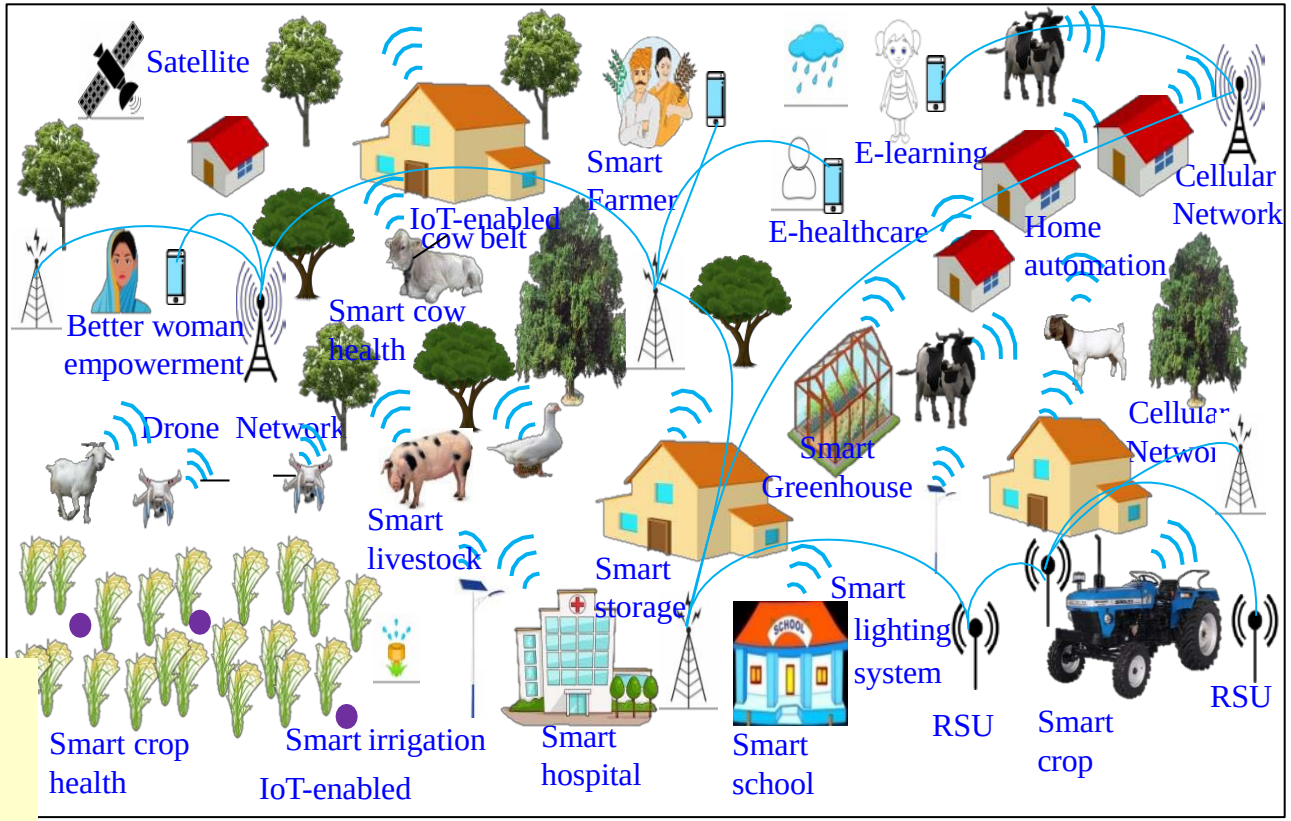
Source: http://edwingarcia.info/2014/04/26/principal/

Smart Cities

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

Smart Villages

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



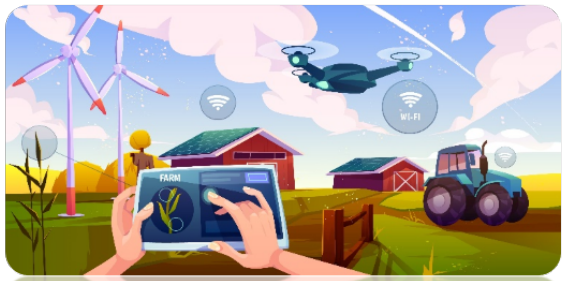
Source; P. Chanak and I. Banerjee, "Internet of Things-enabled Smart Villages: Recent Advances and Challenges," *IEEE Consumer Electronics Magazine*, DOI: 10.1109/MCE.2020.3013244.

Smart Village

Services

- Agriculture
- Irrigation
- Energy
- Livestock
- Healthcare
- Education
- Governance
- Transport

Smart Village

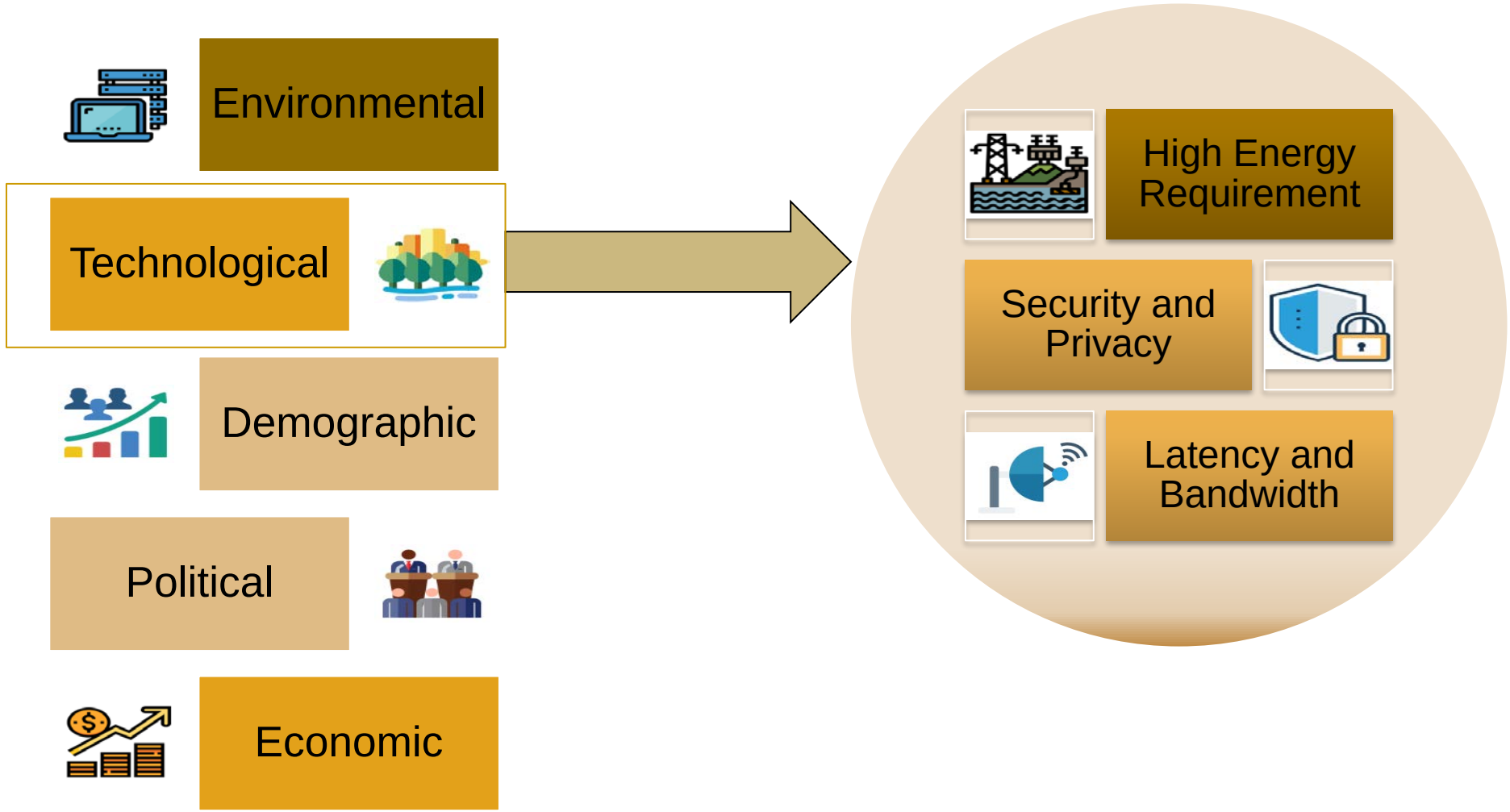


Technologies

- Internet
- Drone Technology
- 5G Technology
- Collaborative Edge Computing
- Green Energy
- Low Power Communication

Smart Village is a paradigm that brings Smart City technologies to the villages but with limitations

Challenges of Smart Village



Security-by-Design (SbD)

- Integration of the cybersecurity early in the design phase, not retrofitted
- Device, circuit, and system-level cybersecurity solutions for robust CPS and smart component design

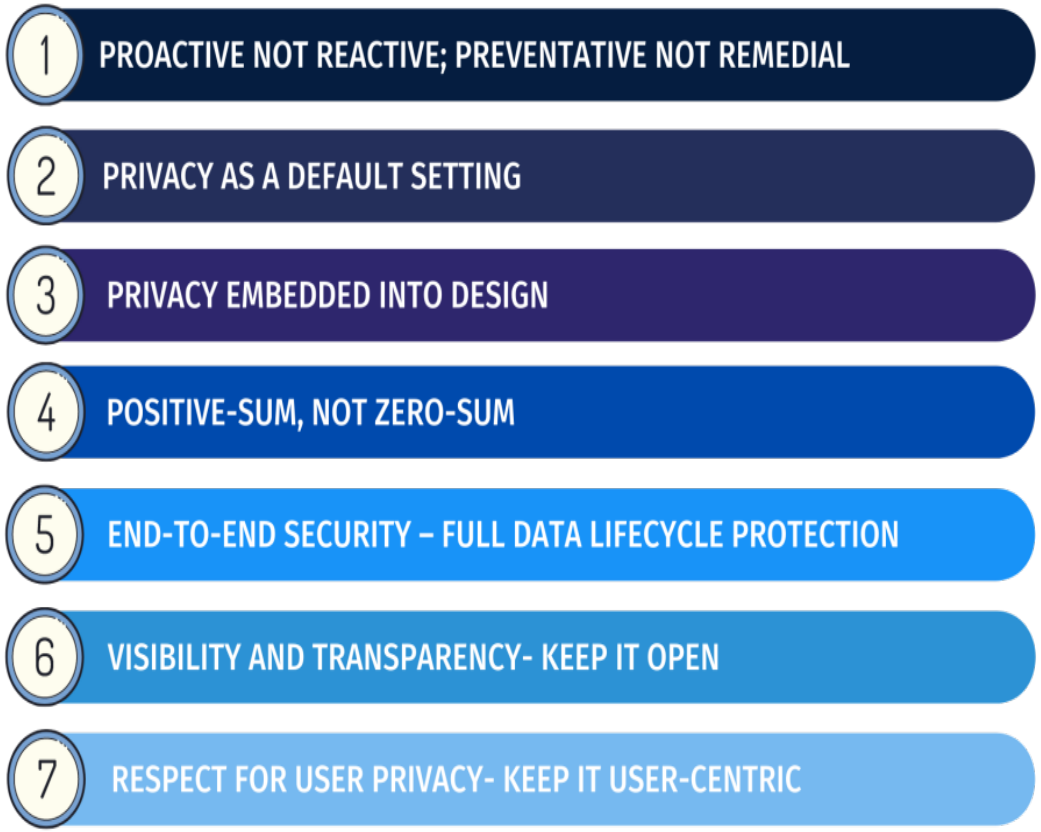
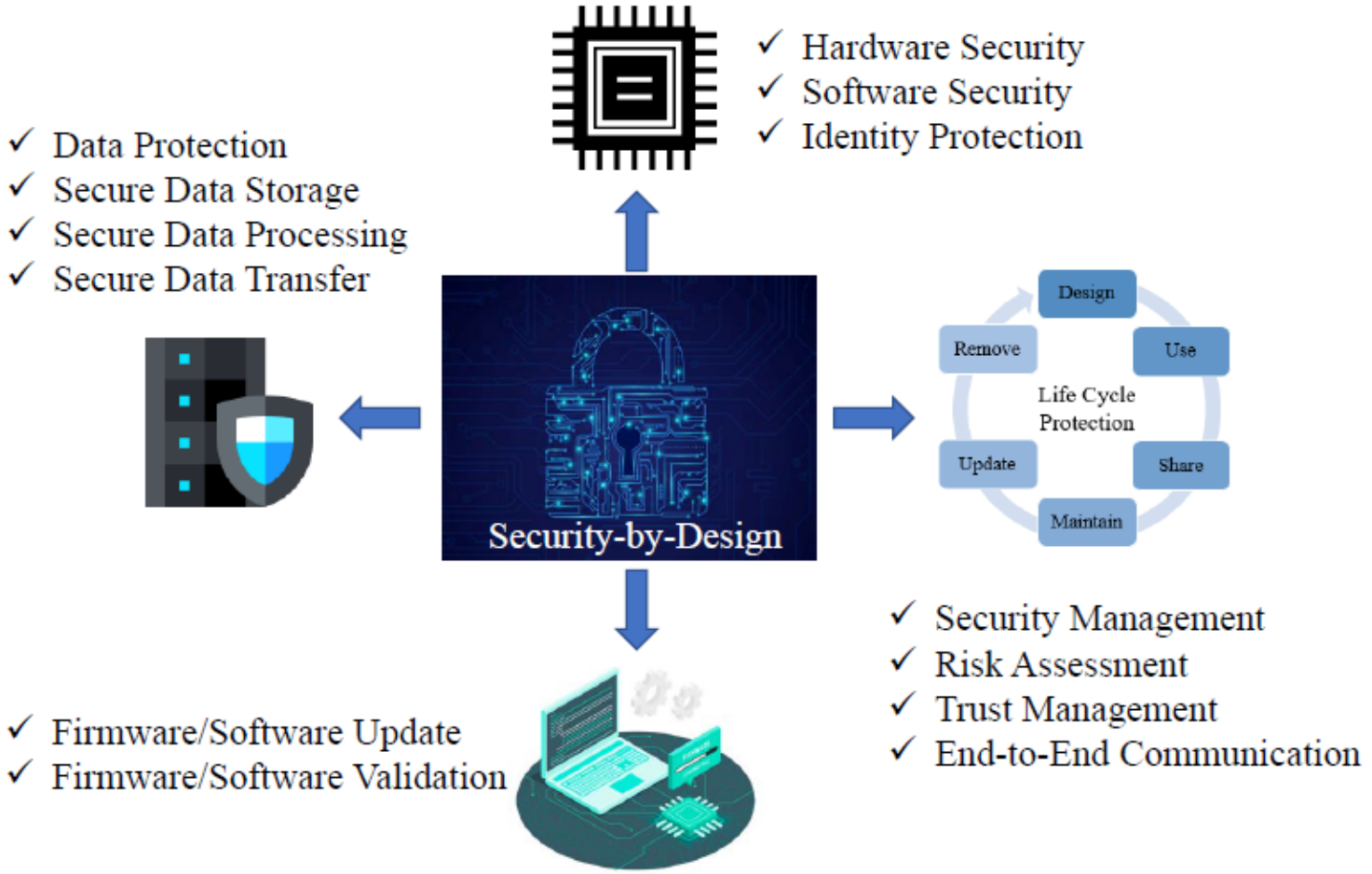


Image Source: https://dataprivacymanager.net/seve-principles-of-privacy-by-design-and-default-what-is-data-protection-by-design-and-default/

Security-by-Design (SbD)



Why SbD?

- The generalization of attacks across all CPS typically ignores the role of Root-of-Trust (RoT) and security perimeter modeling, which are the basis of many SbD approaches

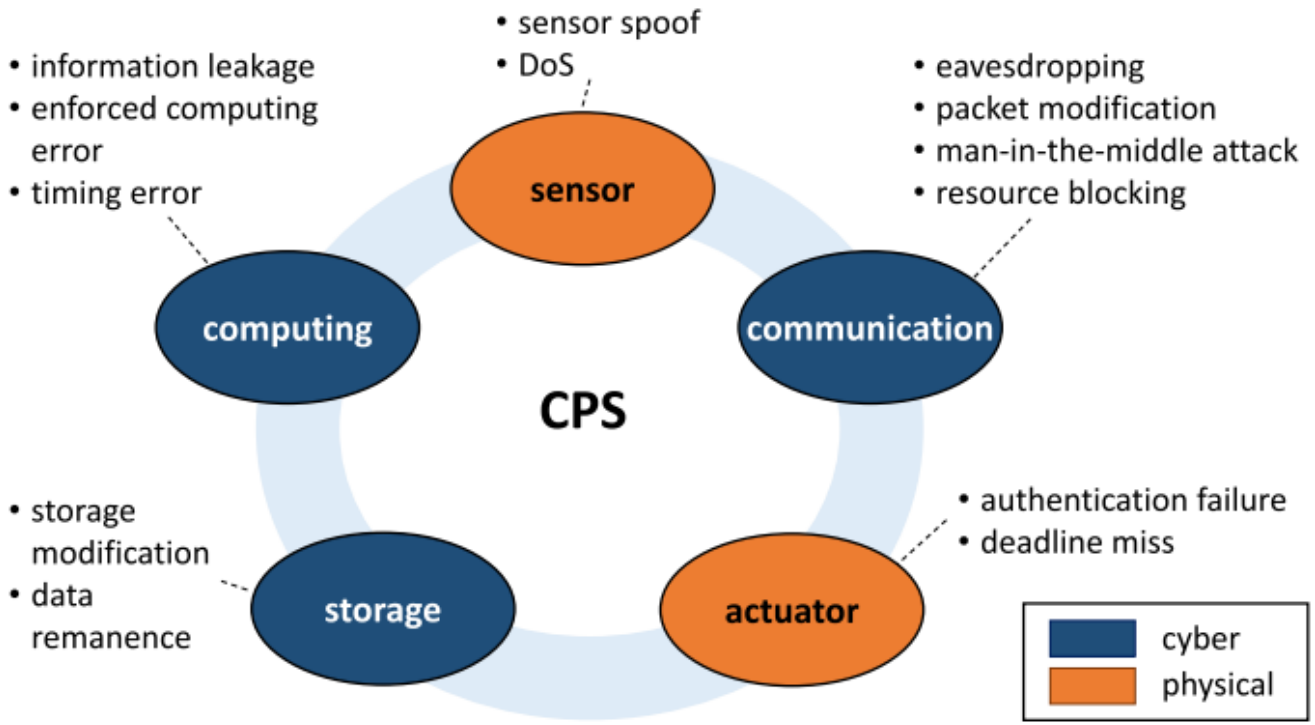
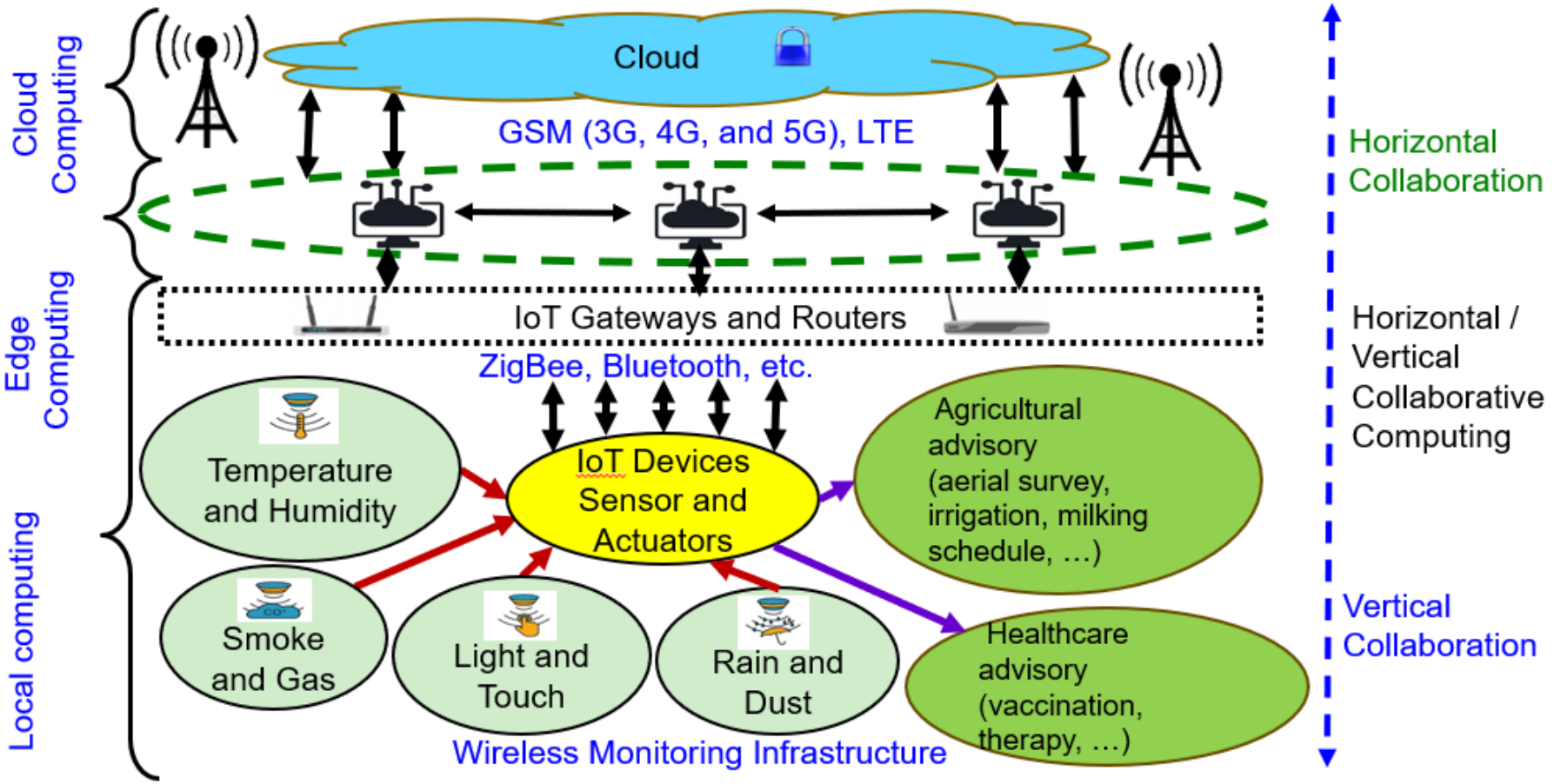


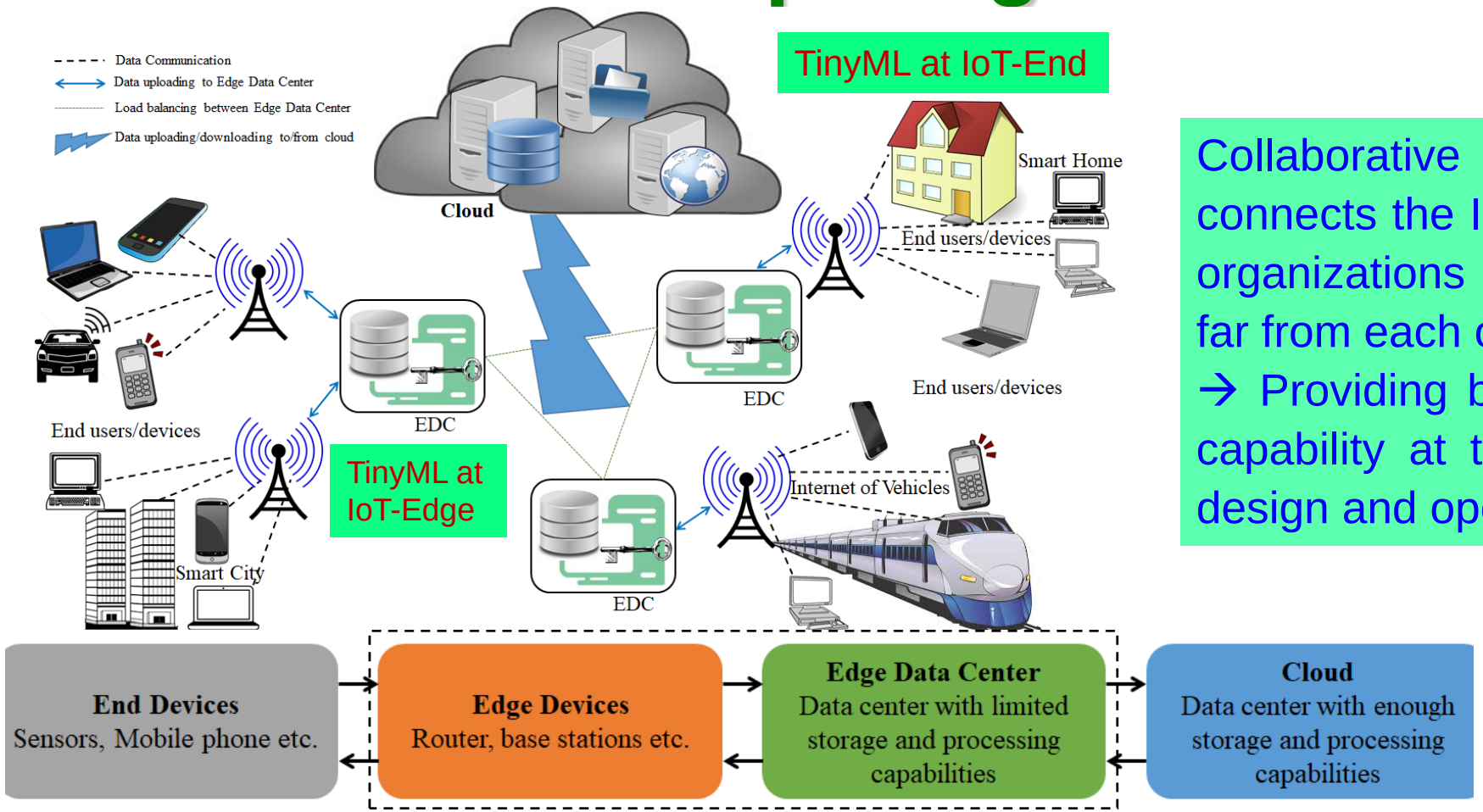
Image Source: A. Chattopadhyay, K. -Y. Lam and Y. Tavva, "Autonomous Vehicle: Security by Design," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 11, pp. 7015-7029, Nov. 2021, doi: 10.1109/TITS.2020.3000797.

Collaborative Edge Computing (CEC)



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 is Cost Effective Sustainable Computing for Smart Villages



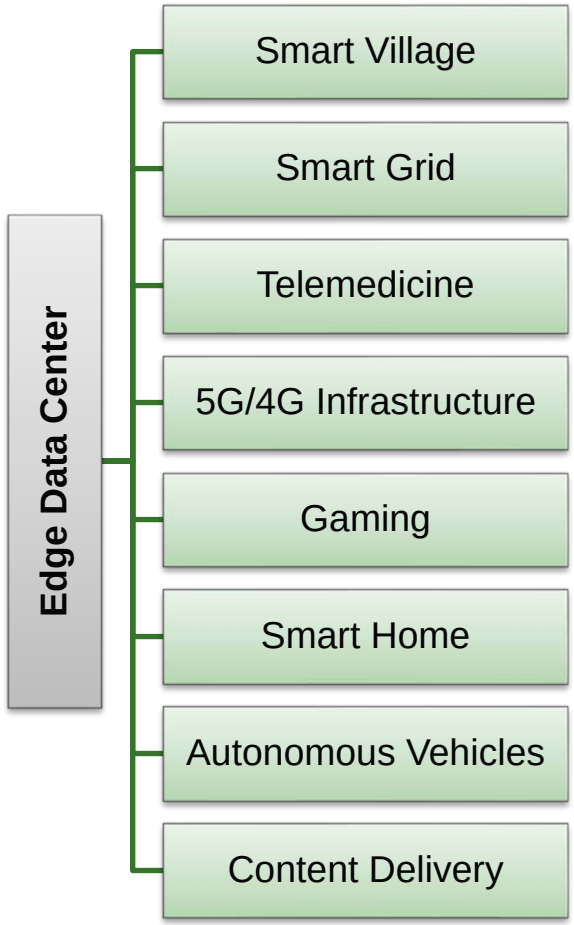
Collaborative edge computing connects the IoT-edges of multiple organizations that can be near or far from each other

→ 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.

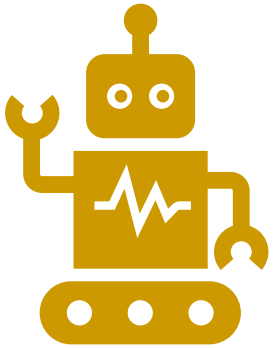
Collaborative Edge Computing (CEC)

- 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



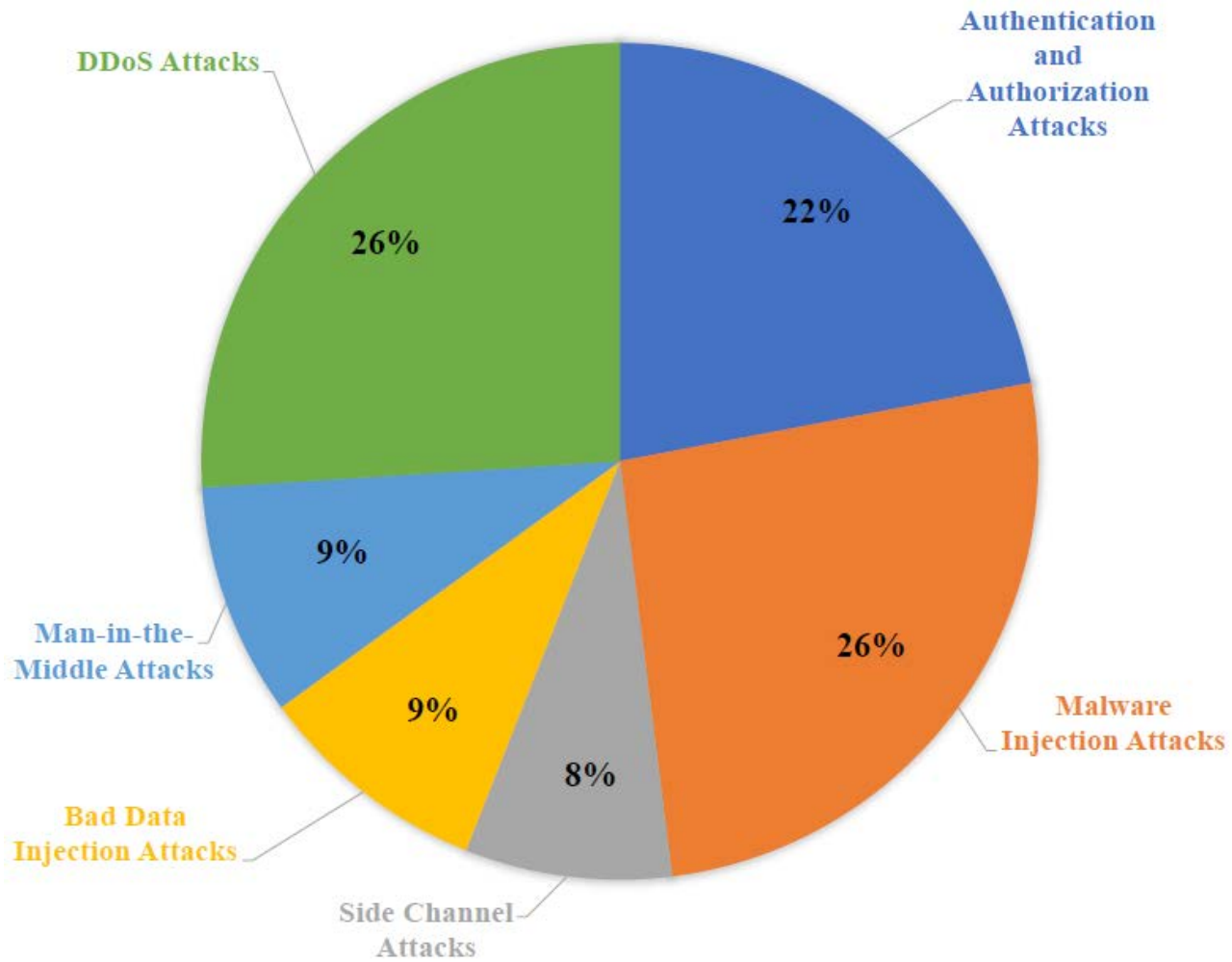
Long-term Vision

Cybersecurity for smart villages based on the SbD principles for secure resource sharing in the CEC environment



AI/ML for Cybersecurity in Smart Villages

Need for Secure Authentication of EDC



Existing Solutions

Symmetric and Key Cryptography

- Advanced Encryption Standard(AES)
- Client & server store a secret key

Asymmetric Key Cryptography

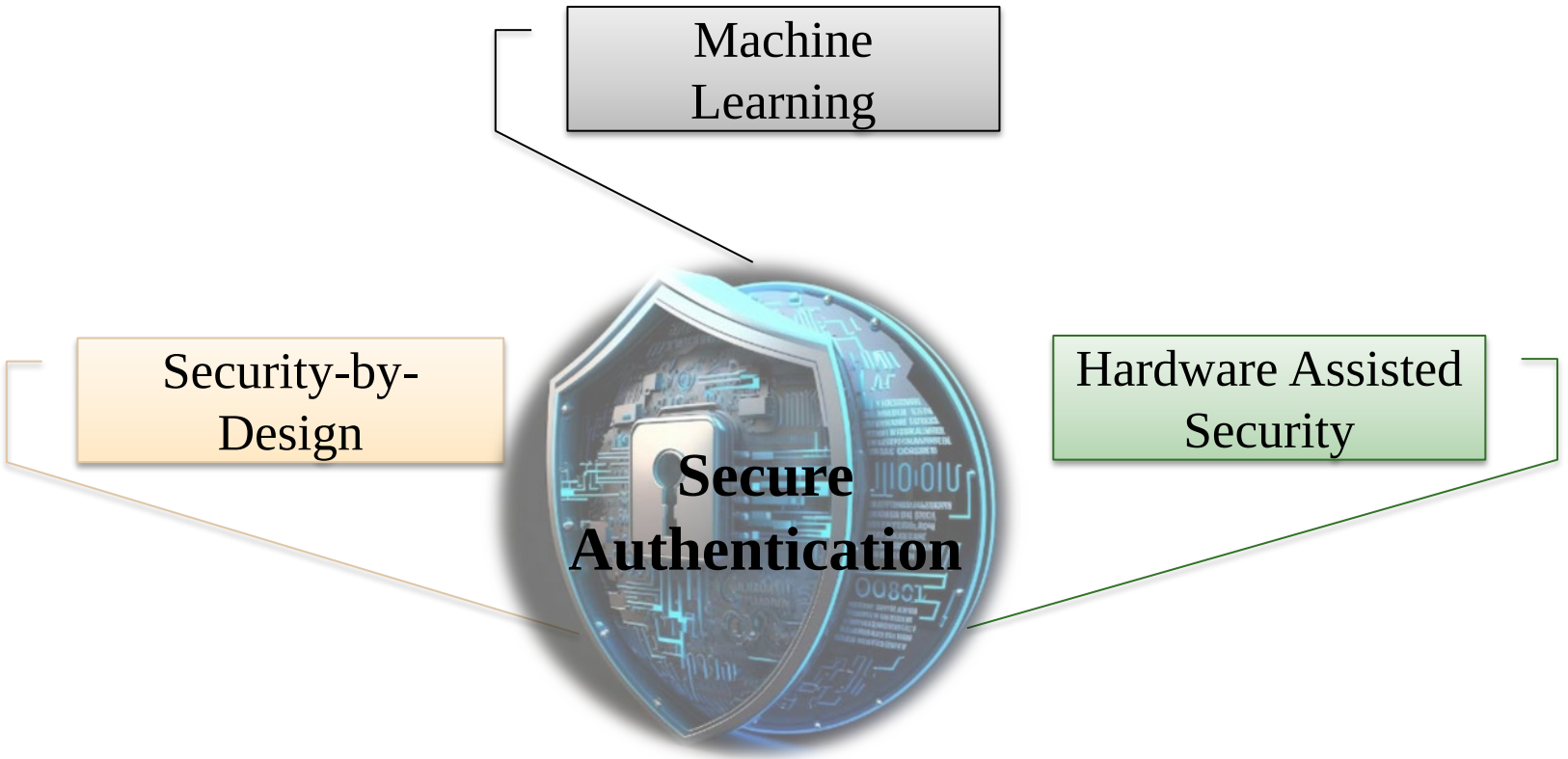
- Transport Layer Security(TLS)
- Secure Sockets Layer(SSL)
- Public Key and Private Key Pairs

Device Localization and Environmental data authentication technique

PUF based authentication techniques

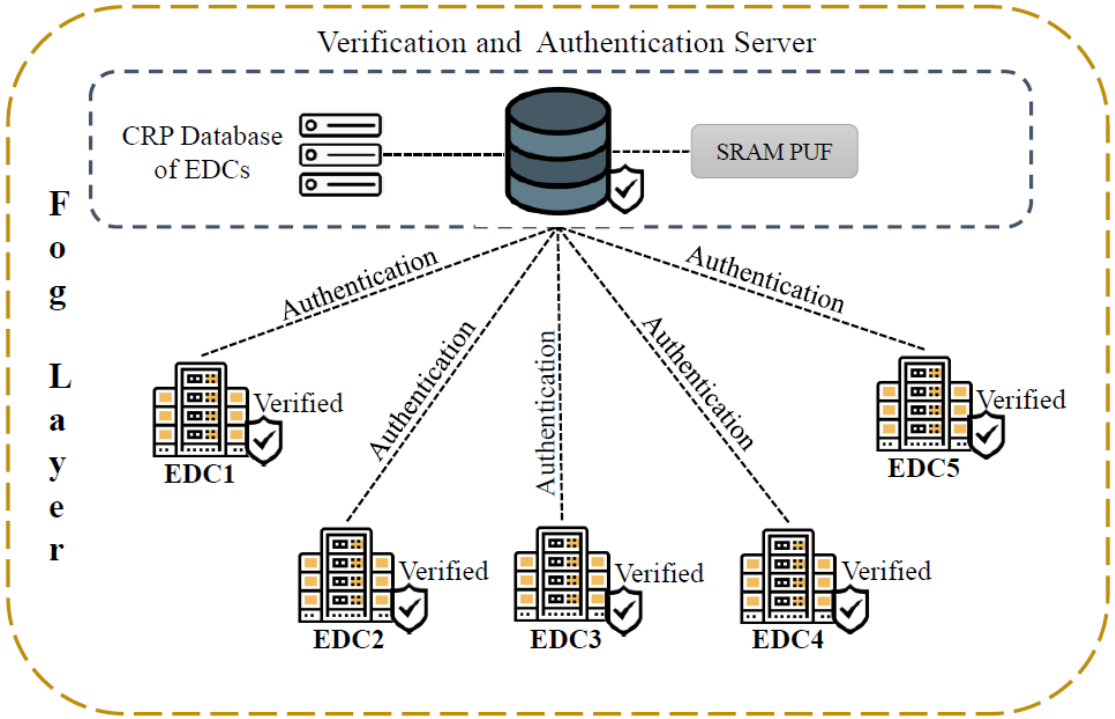
Our Fortified-Edge: The Key Idea

- A lightweight and Secure Authentication scheme for EDCs during load balancing in the CEC environment of smart villages



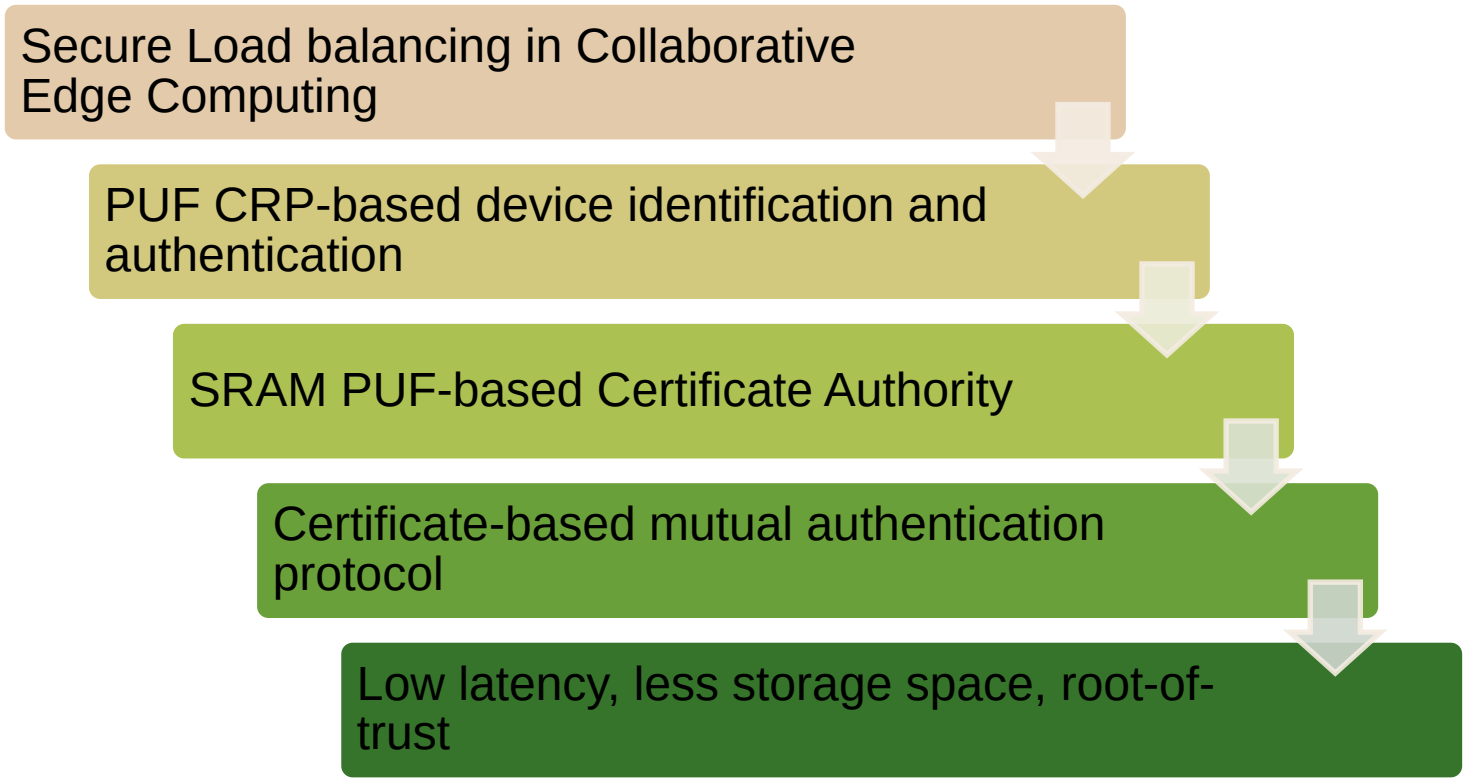
Fortified-Edge 1.0 - The Idea

- CEC enables applications in smart villages through load balancing
- To develop a secure authentication protocol for Load balancing
- Suitable for a smart village environment
- Incorporate Security-by-Design for smart and sustainable security



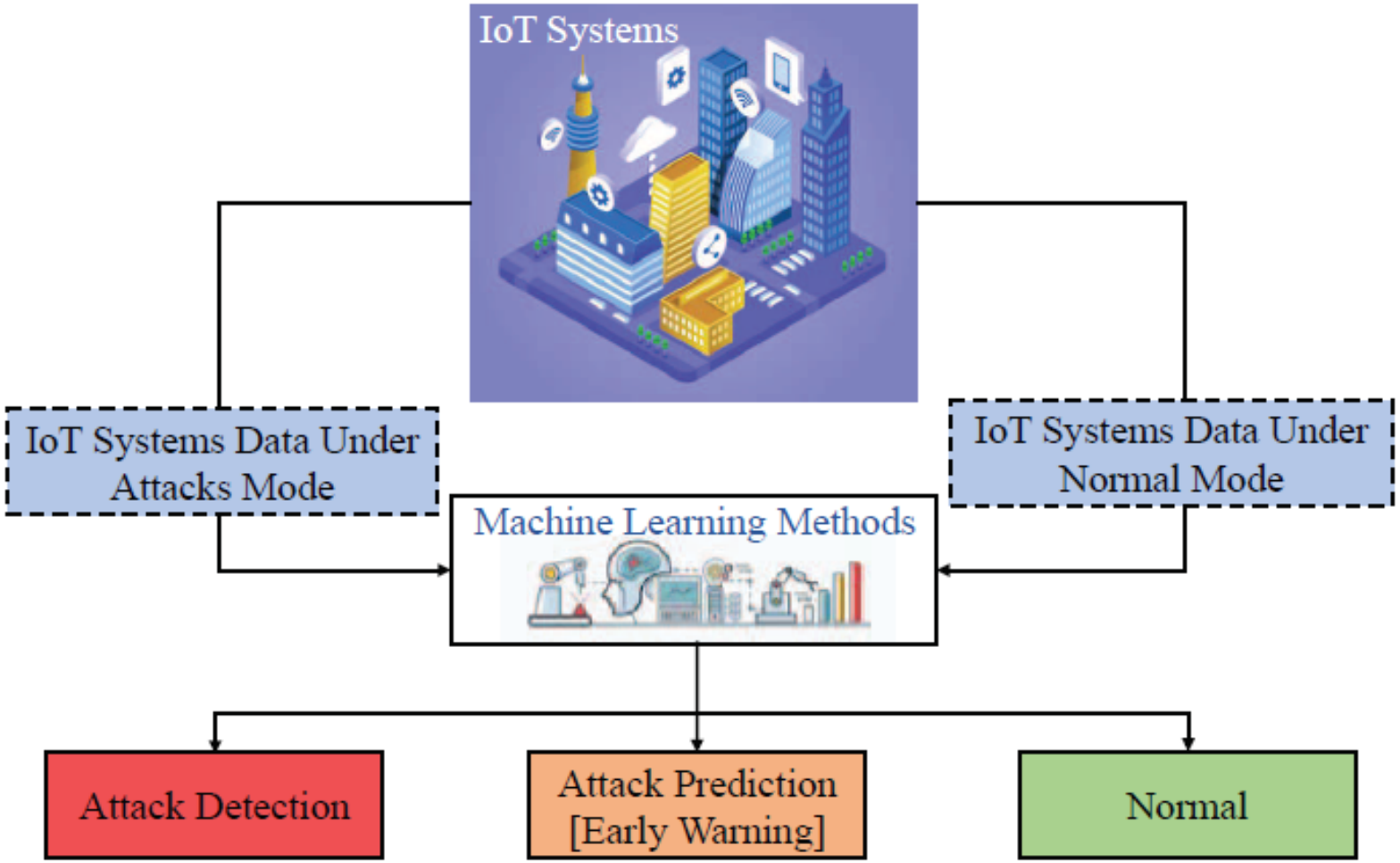
Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 249--254, DOI: https://doi.org/10.1145/3583781.3590249

Fortified-Edge 1.0 - The Approach

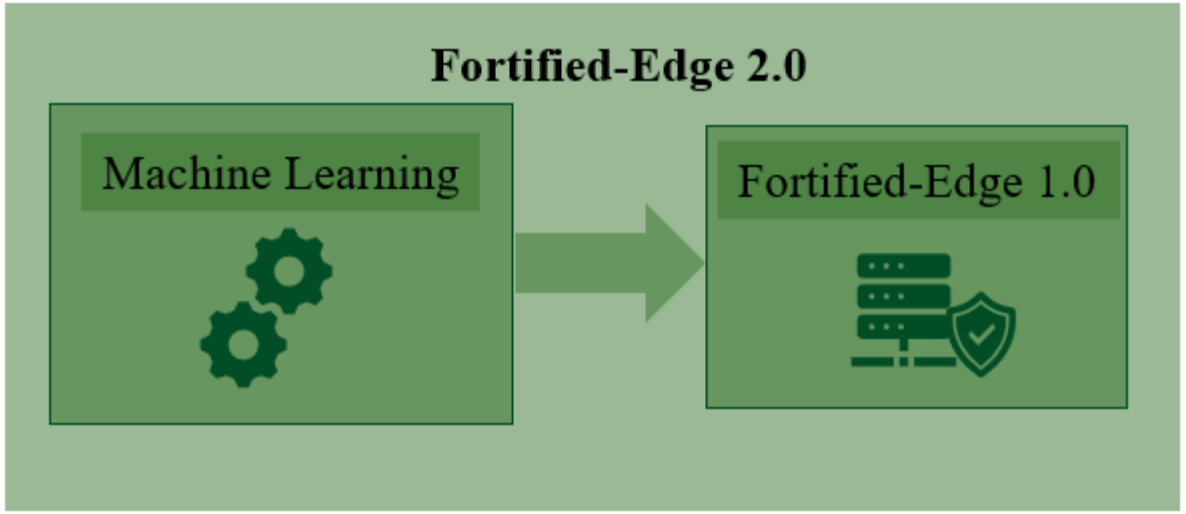


Source: S. G. Aarella, **S. P. Mohanty**, E. Kougianos, and D. Puthal, "Fortified-Edge: Secure PUF Certificate Authentication Mechanism for Edge Data Centers in Collaborative Edge Computing", in *Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI)*, 2023, pp. 249--254, DOI: https://doi.org/10.1145/3583781.3590249.

Machine Learning for IoT Security



Fortified-Edge 2.0 - The Idea



Features

- Secure, Low Latency Authentication
- Device identification
- Intrusion detection
- Attack Prevention
- EDC Monitoring
- Resilient against malicious Requests
- ML model suitable for a smaller dataset

Related Prior Research

Research	ML Model	Application
Yufei et al. [10]	OC-SVM and SVDD	HTTP Anomaly Detection for Edge
Hou et al. [11]	SVM	Network Security of Edge Computing
Oshana et al. [12]	SVM	Attack Detection System
Imtiyaz et al. [13]	SVM	Transformer Monitoring at the Edge
Khosroshahi et al. [14]	3D SVM	DDoS Attack Source Detection
Fortified-Edge 2.0 (Current Paper)	SVM	EDC Authentication and Monitoring in CEC

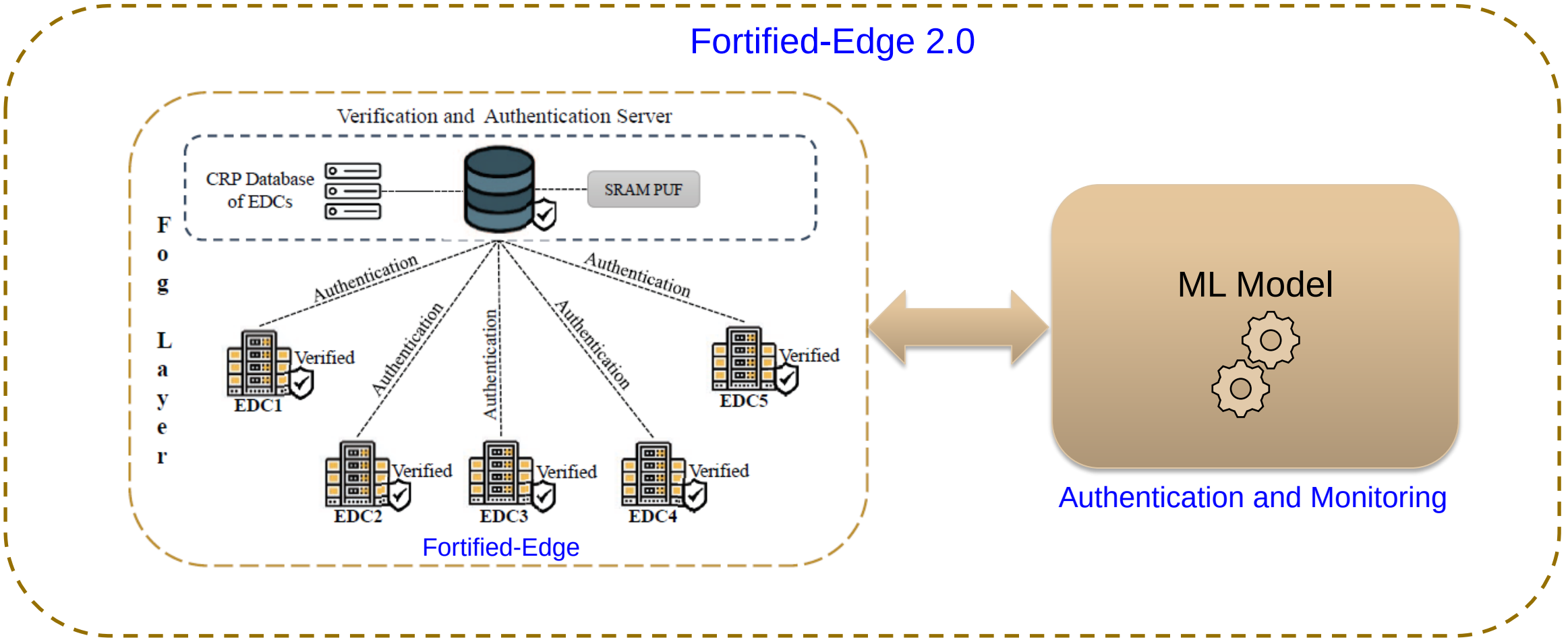
Problems Addressed and Solutions Proposed

- Problems
  - Secure Authentication of EDCs
  - ML methods with low computation
  - Intrusion detection
  - Identity protection
  - ML model with high accuracy in prediction, low error rate, and efficient classification functions
  - Secure authentication through integrated hardware and software
- Solutions
  - Improving the authentication model of Fortified-Edge
  - Supervised ML method using small data size
  - SVM-based ML method for classification and prediction
  - ML for monitoring and authentication of EDC
  - Suitable for computing at the edge

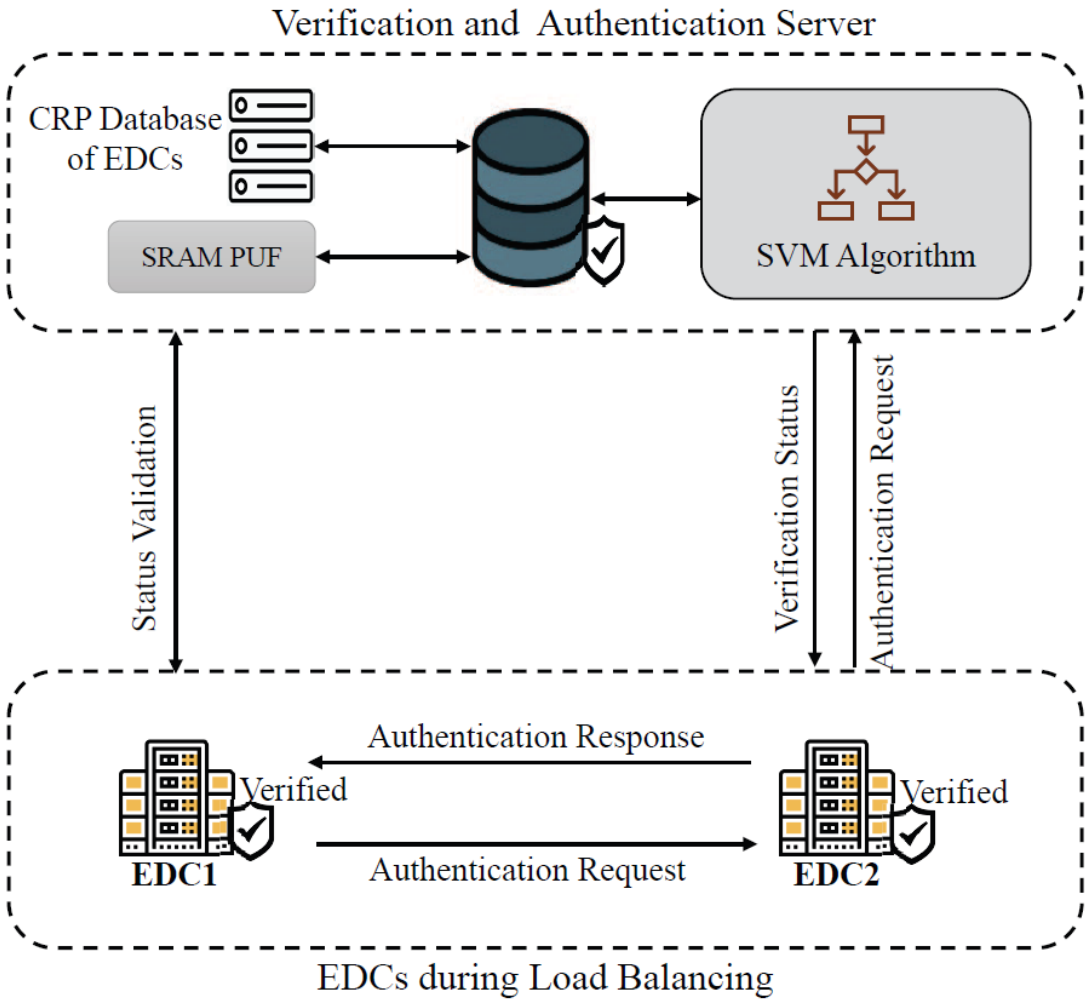
Novel Contributions

- EDC monitoring and authentication through supervised ML
- SVM as an ideal ML method to incorporate at Edge with its available resources
- Selection of a variety of features for training SVM to make it accurate
- Intrusion and malicious authentication detection
- SVM to validate the authentication process and predict invalid authentication requests

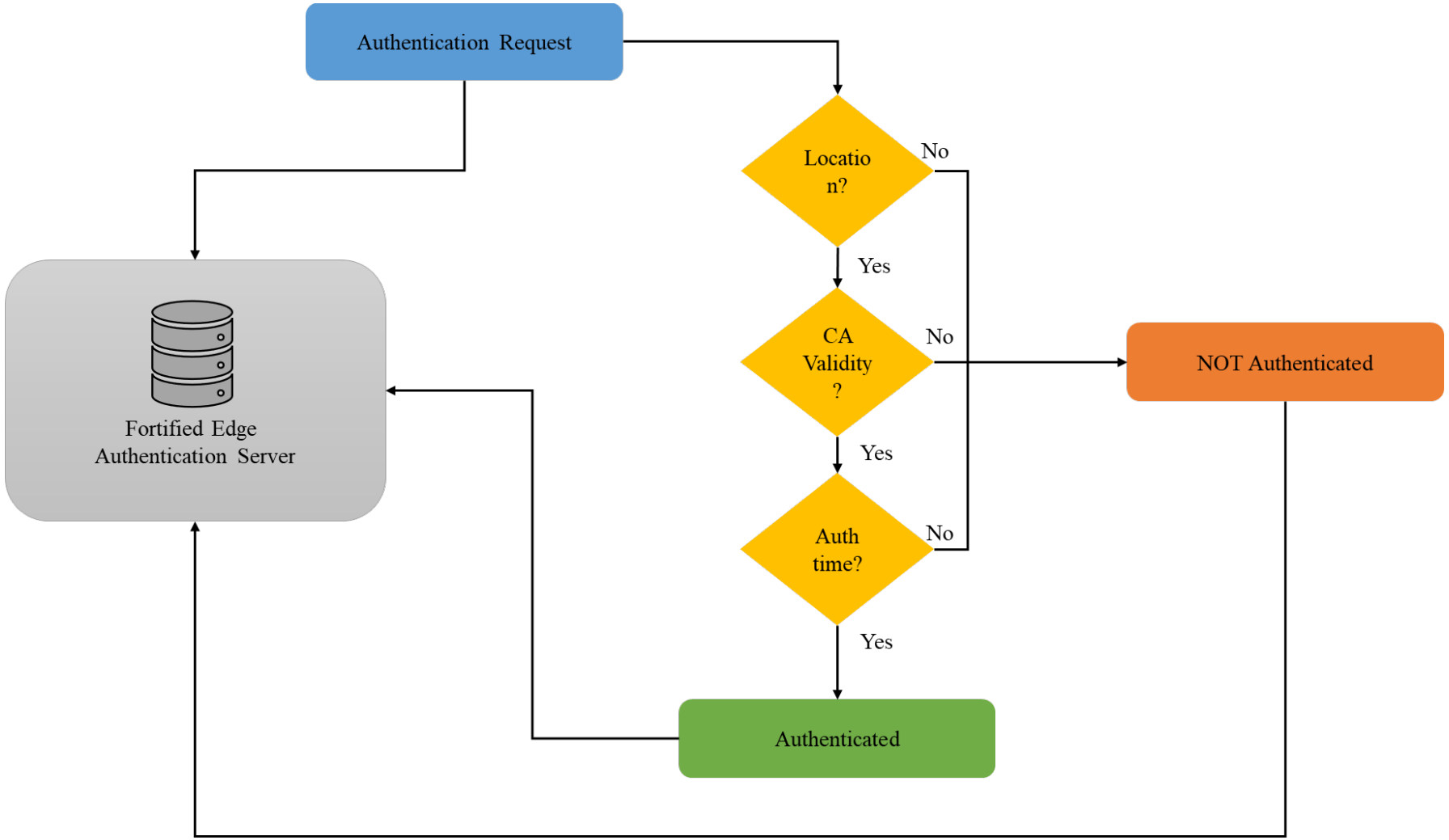
Fortified-Edge 2.0



The Architecture of Fortified-Edge 2.0

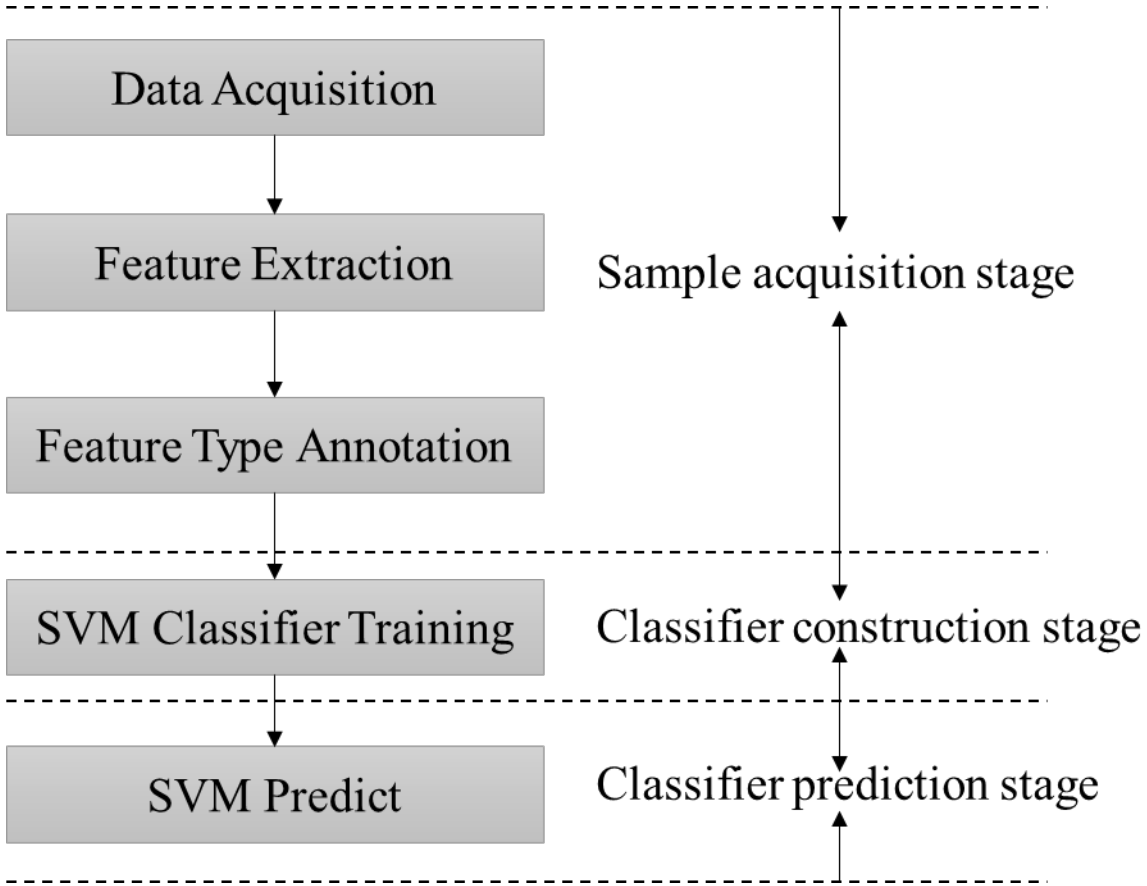


Flow Chart of SVM Algorithm



SVM Algorithm and Features

Basic Function of the SVM Algorithm



Features Considered for SVM Training

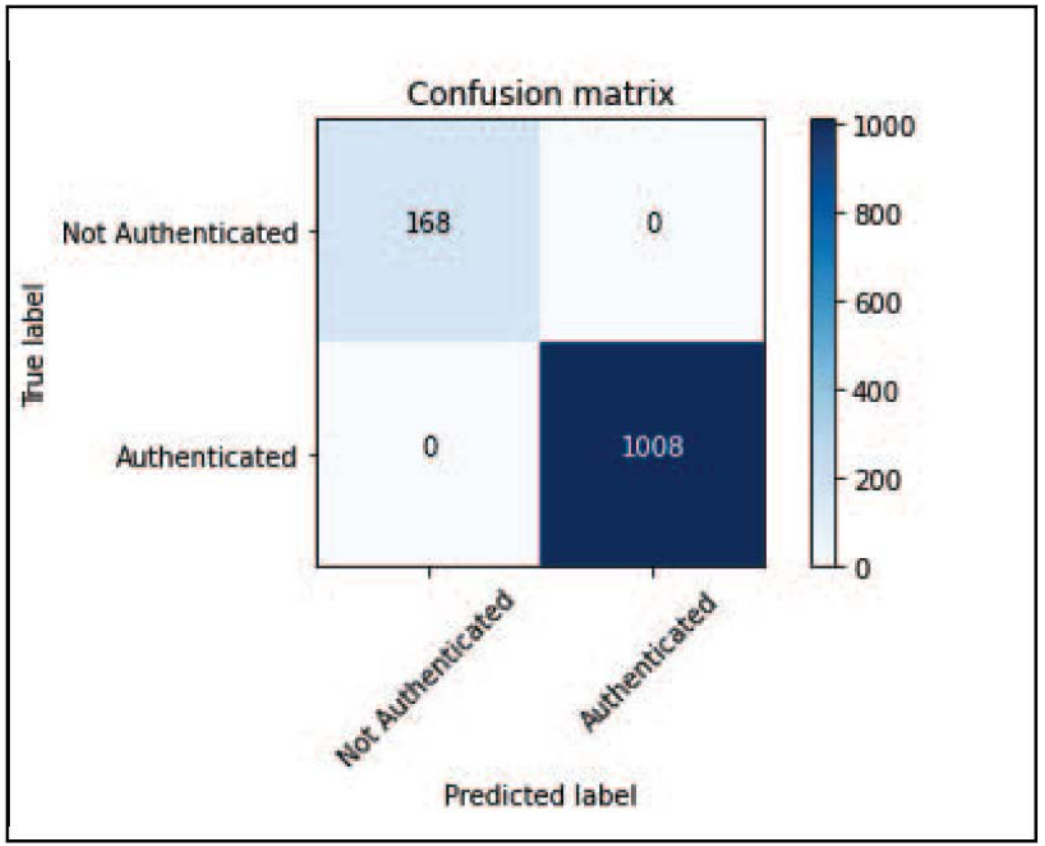
Features	Variable
Site_ID	S_{id}
EDC_ID	E_{id}
EDC_ID_Requestor	E_{idr}
Lattitude_EDC	L_a
Longitude	L_o
Lattitude_EDC_Requestor	L_{ar}
Longitude_EDC_Requestor	L_{or}
Distance	d_r
Certificate_Validity	C_r
Authentication_Time	t_r

Algorithm for EDC data acquisition and SVM training

- Input: Load EDC Site Dataset
- Input: Load EDC Authentication Dataset
- Output: Train the SVM Model to predict the authentic EDC
  - get Authentication Metadata ;
  - get Location Sid ;
  - get CA Validity data cr;
  - get Authentication Time tr;
  - calculate the distance dr;
  - set target as status=0 or 1;
  - split data into Train set and Test set;
  - create a Confusion Matrix;
  - use SVC Classifier for Classification and prediction;
  - If status=1 then
  - Request is authentic;
  - else
  - 13 Malicious Request;
- /* The SVM is trained to predict genuine and malicious authentication requests */

Confusion Matrix

The confusion matrix is created to verify if any misclassification has happened, if there is none, the correct values are seen in the diagonal area



Experimental Analysis

$$\text{Accuracy} = \frac{TP+TN}{(TP+TN+FP+FN)}$$

$$\text{Precision} = \frac{TP}{(TP+FP)}$$

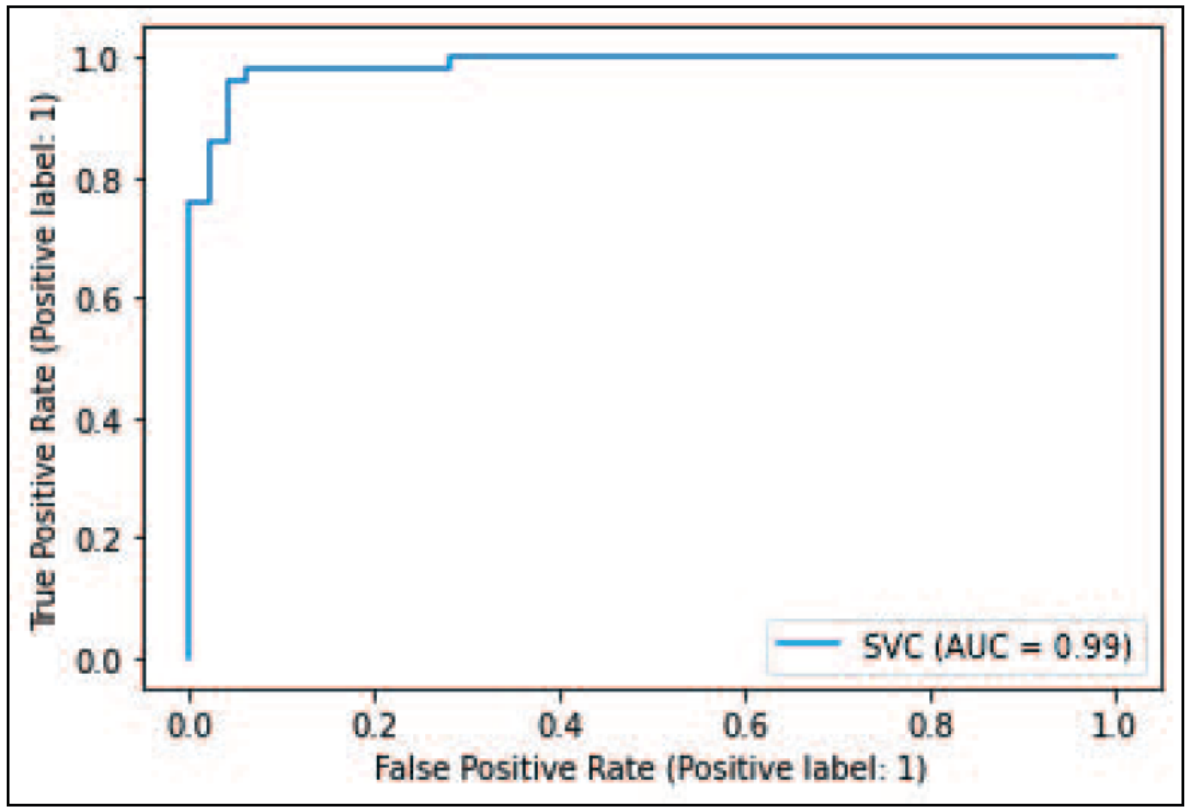
$$\text{Recall} = \frac{TP}{(TP+FN)}$$

$$\text{F1\_Score} = 2* \frac{(\text{Precision}*\text{Recall})}{(\text{Precision}+\text{Recall})}$$

- Metrics for performance evaluation:
  - Accuracy, Precision, Recall, and Area Under the Curve (AUC)
  - Receiver Operator Characteristic (ROC) is a probability curve that plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various threshold values

Experimental Results

If the AUC value is 1, the classifier is able to distinguish between all positives and negatives accurately



Comparison of Results

Research	ML Model	Accuracy	Precision	Recall	AUC	F1-Score
Yufei, et al. [10]	OC-SVM and SVDD	0.983	0.952	0.97	NA	0.961
Hou, et al. [11]	SVM	0.99	NA	NA	NA	NA
Oshana, et al. [12]	SVM	NA	1.0	1.0	NA	1.0
Imtiyaz, et al. [13]	SVM	0.983	0.886	0.995	NA	NA
Khosroshahi, et al. [14]	3D SVM	0.985	0.971	NA	NA	NA
Fortified-Edge 2.0 (Current Paper)	SVM	1.0	1.0	1.0	0.99	1.0

Fortified-Edge 1.0 Vs Fortified-Edge 2.0

- Mutual authentication of EDCs without cloud dependency
- Reducing the latency by edge-based authentication
- PUF CRP for lightweight and secure authentication
- CA-based verification and authentication for faster and more secure process
- No storage space complexity

- No cloud dependency
- ML for attack detection, intrusion detection, malicious request detection
- ML model suitable for processing at edge
- Improved security over Fortified-Edge 1.0

Conclusion

- Fortified-Edge 2.0 aims at designing a security application that follows the principles of Security-by-Design (SbD)
- The research is an integrated security solution that combines the Hardware-Assisted Security (HAS) feature of the PUFs in the SRAM PUF-based CA model
- Machine Learning to improve the secure authentication process at the edge
- SVM model with linear classifier is 100% effective in predicting the valid authentication requests
- Efficient in Intrusion Detection at the Edge

Future Research

- SVM can be used for detecting communication-related anomalies at the edge.
- Prevention of communication/network attacks while considering load sharing in EDC.
- Consideration of vertical and horizontal paradigms of CEC for effective SbD.

Thank you!