DRAM-Based Authentication Using Deep Convolutional Neural Networks

Michael Yue
Santa Clara University

Nima Karimian
San Jose State University

Wei Yan
Washington University in St. Louis

Nikolaos Athanasios Anagnostopoulos
University of Passau

Fatemeh Tehranipoor
Santa Clara University

***Abstract*—Authentication is the act of proving that an integrated circuit (IC) is not counterfeit. One application of a physical unclonable function (PUF) circuit is to authenticate the identity of the chip using raw bits of the memory. However, several previous works present machine learning-based modeling attacks on PUFs. To alleviate this issue, we propose a novel authentication scheme involving unique DRAM power-up values using a deep convolutional neural network (CNN). This methodology eliminates the need for PUFs and can authenticate DRAM technology accurately with a neural network. Our approach converts raw power-up sequence data from DRAM cells into a two-dimensional (2D) format to generate a DRAM image structure. This makes it harder for an adversary to use machine learning since there is no PUF to exploit the weaknesses. Then, we apply deep CNN to DRAM images to extract unique features from each chip and classify them for authentication. Our method "DRAMNet" achieves 98.84% accuracy and 98.73% precision. The proposed technique has the advantage of a faster authentication**

Digital Object Identifier 10.1109/MCE.2020.3002528
Date of publication 15 June 2020; date of current version 10 June 2021.

while eliminating the need for costly error correction mechanisms and CRPs. To the best of our knowledge, this is the first method to authenticate ICs using DRAM and CNN.

Among various techniques to enhance the security of integrated circuits (ICs), physical unclonable functions (PUFs) are very popular as they are easy to implement, hard to predict, and difficult to duplicate. The idea of a silicon PUF was first proposed by Gassend *et al.*.[1] They developed the first silicon PUFs through the use of intrinsic process variability (PV) in deep submicrometer ICs. PUFs extract the intrinsic PV of the manufacturing of silicon devices to produce unique, random, and unclonable digital responses. Generally, a PUF is a function that is embodied by a physical device, which maps inputs to outputs, creating challenge-response pairs (CRPs).[1] In a PUF-based authentication scenario,[6] one of the inputs for which a corresponding output has been recorded and kept secret is provided as an input to the PUF circuit. The output of the PUF circuit is compared with the corresponding stored output. If they match, the chip is authenticated. Upon every successful authentication of a given IC, a set of CRPs is potentially revealed to the adversary. This means that the same CRP cannot be used again. If the adversary can learn the entire set of CRPs, they can create a model of a counterfeit IC. The most plausible attack we have found against PUFs is the model-building attack.[4] Powerful machine learning tools are used to develop such attacks since it can gather CRPs efficiently and effectively. Model building attacks are powered by machine learning tools, which can gather CRPs efficiently and effectively.

In this article, we propose a new authentication method (DRAMNet) that is based on the intrinsic properties of DRAM power-up values using a deep CNN architecture. DRAMNet is another way of authenticating an integrated circuit as compared to other works. In our previous work[2] on DRAM PUFs, we have implemented three COTS DRAM memories and tested/collected their power-up values under various environmental conditions, i.e., normal condition, high temperature, low temperature, high voltage, low voltage and aging. For reliable authentication, we require that environmental variations and measurement errors do not produce so much noise that they hide interchip variations. Our new proposed scheme, DRAMNet, works based on a deep learning classifier using DRAM images; unlike traditional PUFs where CRPs are needed for authentication. We can authenticate DRAM in this way without needing PUFs and only using the raw bit values from memory. Basically, DRAM images are constructed using the two-dimensional (2D) structure of the memory cells at power-up. Then, we apply the CNN to extract unique features from each DRAM in order to distinguish each device. This method allows for the authentication of an IC without the need of CRPs and PUFs. DRAMNet is also resistant against a model-building attack because an adversary would need access to the entire memory space of a device to construct a model. An attacker would need significantly more resources to construct a model because they would need the entire DRAM memory space. In this article, we describe the notion of physical unique features and argue that this new method of authentication can be implemented using DRAMs. To summarize, our contributions are as follows.

- We convert the raw power-up sequence data from DRAM cells into a 2D format and then generate DRAM images.
- We apply a deep CNN scheme to the DRAM images to classify each device for authentication purposes.
- We examine the quality of the proposed DRAMNet model based on various metrics such as F-score, Precision, Recall, and Accuracy.
- We compare the proposed model against two other CNN models, namely AlexNet and VGGNet.
- We eliminate the need of PUFs using the CRP generation process by considering the entire memory space for authentication.

The remainder of the article is as follows. First, we conduct a thorough review of the literature and perform detailed profiling to locate any limitations. Then, we describe the DRAM

architecture and properties in the "DRAM Description and Properties" section. In the "DRAMNET Methodology" section, we outline the DRAMNet technique and compare against PUF-based authentication. The "Experimental Setup and Results" section illustrates experimental results. The Applications of the proposed authentication scheme is presented in the "Potential Applications of DRAMNET" section. Our work concludes in the "Conclusions and Future Work" section.

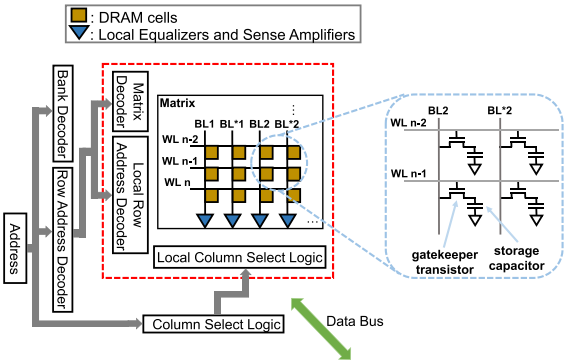

Figure 1. Internal DRAM organization.

LITERATURE REVIEW

PUFs can be broadly categorized into strong and weak types. A strong PUF can accommodate a very large number of challenges and produce corresponding responses. We note that previous works have most often utilized machine learning as a way to attack the so-called "strong" PUFs[4,5] that were based on the physical variations of delay elements. On the other hand, weak PUFs hold a very limited number of challenges, often only one. Memory-based PUFs are a notable example of this type. In particular, security primitives based on the physical characteristics of DRAM have been examined in considerable detail. Recent works have investigated the potential of a number of characteristics of DRAM cells to serve as the basis for the implementation of security primitives. The power-up values of the DRAM cells,[2] their data remanence and data retention characteristics,[3] as well as their latency variations, are all various physical characteristics of DRAM modules. Although a number of related works exist regarding the usage of DRAM as a security primitive, this is the first work that connects the unique characteristics of DRAM cells with the emerging field of machine learning. Strong PUFs and XOR PUFs are also vulnerable to reliability-based modeling and approximation attacks.[14,15] These types of attacks are developed to target systems that are generally secure against machine learning attacks. These techniques analyze the logical and functional structure of PUFs and build models using that analysis. A logical structure of the PUF is created with a neural network, which compromises the PUF's integrity. While CRP-based PUF methods are vulnerable to machine learning attacks and other modeling-based attacks, DRAMNet utilizes machine learning and CNN to significantly limit the use of CRPs. Leveraging the nonlinear behavior of cellular neural networks to create a PUF has so far been presented only in one previous work.[9]

DRAM DESCRIPTION AND PROPERTIES

DRAM is a memory module that is most often an inherent component of modern computer systems. Therefore, DRAM-based security primitives tend to be highly cost-efficient and practical. Additionally, as contemporary DRAM modules are of a significantly large size (usually of some gigabytes), they allow for the extraction of a relatively large number of unique features, based on their physical characteristics. Due to their size difference, DRAMs offer a larger amount of entropy compared to SRAMs.[2] As shown in Figure 1, DRAM modules tend to be organized in a complex way, consisting of banks of data that are organized into arrays of several matrices of cells. Each individual DRAM cell consists of a gatekeeper transistor and a storage capacitor, and stores a single bit, based on the charge state of its capacitor. In a matrix of cells, all the gates of the transistors of DRAM cells of the same row are connected to a single Word-Line (WL), which enables access to all the cells of that row at the same time. In a similar fashion, the cells of each column of a matrix of cells are all connected to a single BitLine (BL or BL*), which is used to gain access to the charges of their capacitors. As each wordline allows access

to all the cells of a row at once, the logical values of all the cells of a single row can be read or written at the same time using the bitlines. For this reason, adjacent bitlines are usually working as a pair; when one bitline (BL) is charged or discharged, the other (BL*) is, respectively, discharged or charged. Reading or writing a particular cell, or row of cells, is done by charging up the corresponding wordline and measuring the differences in the charge of the corresponding bitline(s) through sets of equalizers and sense amplifiers that connect adjacent bitlines. The logical value of a cell is determined based on whether the charge of its corresponding capacitor is above or below a certain threshold voltage value. Additionally, as the capacitors are not ideal, the charge stored in them slowly leaks away, therefore, they need to be frequently recharged, through an operation known as *DRAM refresh*.

DRAMNET METHODOLOGY

Generally, DRAMNet is a technique that uses the advantages of a neural network to authenticate an IC. Instead of generating CRPs from a PUF circuit, DRAMNet can detect the characteristics of DRAM using images and identify unique ICs with deep learning methods. The step-by-step procedure of the DRAMNet technique is presented below.

DRAM Cells 2-D Structure and Images

In this work, we generate unique features from DRAM modules, in order to authenticate a device. The advantage of using memory as a source of authentication is that DRAM is present on most computer systems and can be used for generating device-specific signatures without requiring any additional circuitry or hardware. In our previous experiments in the article by Tehranipoor *et al.*,[2] we utilized three 1-Mbit DRAMs (DRAM1, DRAM2, and DRAM3). The power-up values of each DRAM were measured under both normal condition and various environmental and other variations. After capturing raw cell power-up values, we convert our binary data into a 2D structure, consisting of multiple rows and columns. For example, for each measurement of our 1-Mbit DRAMs, a 2D structure of 1024 rows by 1024 columns is created. We then use these 2D structures as inputs to produce DRAM images for the deep CNN architecture. The reason of using 2D structures is their suitability for deep CNN, since 1D sequence data downgrade the performance of the authentication. Furthermore, we converted these 2D structures of power-up measurements into a gray-scale images using functions in MATLAB, as shown in Figure 2. The proposed CNN architecture is discussed in the following section.

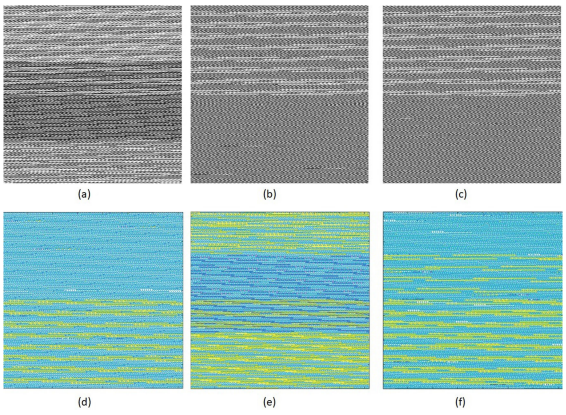

Figure 2. Converted images corresponding to each DRAM (a)–(c). Contour plots for the DRAM images (d)–(f).

Applied CNN Architecture for Authentication

Our classification method consists of the following steps: data acquisition, DRAM data preprocessing, and CNN classification. Deep learning models generally contain input, hidden, and output layers. Our designed CNN model can be divided into inputs (DRAM images), convolution methods, pooling layers for reducing the size of images, fully connected layers for classification, and output layers (labels for each DRAM). The DRAM cells power-up data were collected from COTS memories in the article by Tehranipoor *et al.*[2] First, we transform every single DRAM measurement into a 1024×1024 gray-scale image for CNN inputs. Each DRAM image is entered into an input layer to be then classified. Second, the convolution layer is connected to the DRAM image and calculates the dot products between this connected area and its own weighted value. Third, the pooling layer performs down-sampling per dimension and

Table 1. Architecture of the proposed CNN model.

	Type	Kernel size	Stride	#Kernel	Input size
Layer1	Conv2D	3 × 3	1	3	1024 × 1024 × 1
Layer2	Conv2D	3 × 3	1	64	1024 × 1024 × 3
Layer3	Pool	2 × 2	2		1024 × 1024 × 64
Layer4	Conv2D	3 × 3	1	128	512 × 512 × 64
Layer5	Pool	2 × 2	2		512 × 512 × 128
Layer6	Conv2D	3 × 3	1	192	256 × 256 × 128
Layer7	Pool	2 × 2	2		256 × 256 × 192
Layer8	Full			2048	128 × 128 × 192
Layer9	Full			2048	2048
Layer10	Out			3	2048

outputs the decreased volume. Then, in the fully connected layer, all nodes are interconnected, and the result of each node is calculated by the matrix multiplication of the weight and adding a bias to it. Finally, in the output layer, all classes are converted into a probability via the Softmax function and are classified according to the highest probability. The architecture of our CNN model is listed in Table 1. Table 1 describes the detailed architecture of our CNN model. The raw bit values of the DRAM are converted into an image and processed through DRAMNet. The features that result from DRAMNet, the image itself, and the raw power-up values of that DRAM are stored in a trusted database. Figure 3 shows the procedures utilized in DRAMNet authentication, as well as the relationship between the trusted and untrusted environments. Similar to PUF-based authentication, DRAM authentication operates in both a trusted and untrusted environment. The same process occurs in an untrusted environment except the features are not stored in a database. Instead, those features are compared to the ones in the database and if they are the same, the IC is authenticated.

We applied the following techniques and metrics to our CNN architecture. First, in order to reduce overfitting in the training phase, regularization is applied.[10] Second, the CNN classifier was optimized in order to reduce overfitting and improve classification accuracy. Finally, a cost-function is used to evaluate the effective performance of training neural networks. The cost-function is a cross-entropy function that is used to minimize the

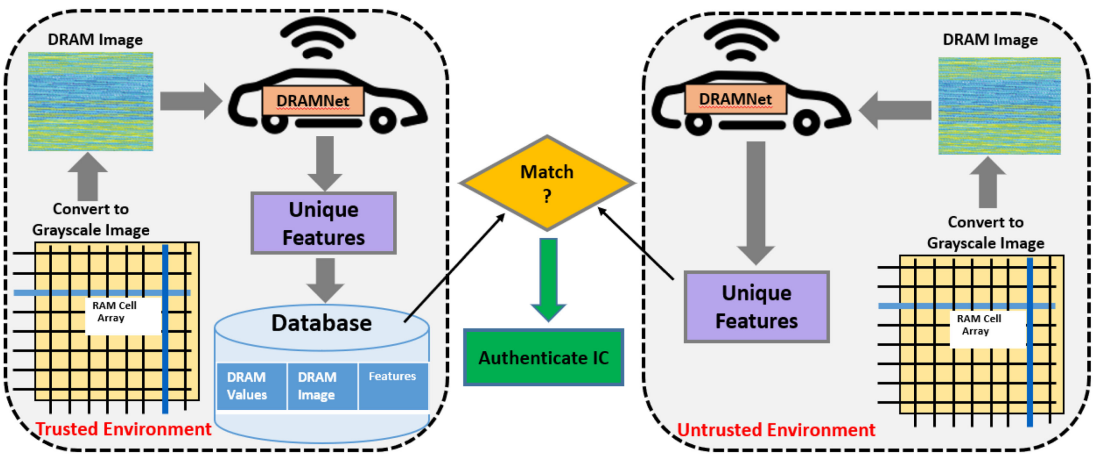

Figure 3. DRAMNet authentication scheme. DRAMNet generates unique features from DRAM memory to verify IC.

difference between the given trained DRAM image and the desired output.

PUF Versus DRAMNet Authentication

In PUF-based authentication, first a subset of the possible (input, output) pairs for the PUF are determined by providing different challenges to the PUF circuit and recording the corresponding responses. The challenges are chosen so that the PUF circuit uses a variety of combinations of the separate physical characteristics (physical states). The challenges and responses of the PUF circuit are kept secret, until they are used. This is also referred to as the enrollment stage. The challenges and responses are stored in a trusted database until the verification phase. At the time the identity of the chip is to be authenticated, one of the challenges for which a corresponding response has been recorded and kept secret is provided as a challenge to the PUF circuit. The response of the circuit is then compared with the stored corresponding response. If they match, the authentication is successful. This is also known as the verification phase. The previously enrolled challenges from the database are applied to the PUF and compared to the enrolled output. Upon every authentication of a given chip, a CRP is potentially revealed to an attacker. The same CRP is preferably not reused. A database of CRPs is maintained by an entity that wishes to identify the chip. In the article by Tehranipoor *et al*,[2] DRAMs were tested under various conditions and raw startup data were collected. These raw data values do not act as a PUF. A proper bit selection algorithm was used to generate PUF ids from the raw data values.

In DRAMNet-based authentication, there are no CRPs needed to authenticate an IC. First, the values of the entire memory space are gathered from a user's IC. A subset of the memory space is converted into a gray-scale image. Next, the image is processed through the DNN to determine unique features of the IC. The features generated from the DNN are later compared to the features in a trusted database. If those features match, then the IC is authenticated. DRAMNet is also resistant against machine learning attacks since an adversary needs the entire memory space to build a model. The memory space is already difficult to acquire and even if an adversary can obtain the memory space, it is inefficient to use a model-building attack. Such attacks have already proved to be effective against PUF-based authentication schemes so using DRAMNet limits the power of those attacks. There is also the concern that an attacker can gather the images from the trusted database. This issue can be handled with basic encryption algorithms such as advanced encryption standards (AES). Other security algorithms can be applied to protect the images at this part of the authentication scheme.

Specifically, DRAMNet-based Authentication has the following advantages.

- The time needed to generate unique features and store them into a database is much less than the enrollment time required for the enrollment of CRPs for DRAM PUF-based authentication.
- The number of raw bit values required for generating unique features are significantly fewer than the number of samples required for the enrollment of a "strong" PUF that provides multiple CRPs. Additionally, the CNN approach does not require an error correction mechanism, unlike "weak" PUFs, which only provide a noisy CRP and, therefore, require error correction.
- Since the DRAMNet scheme is based on a deep CNN architecture, we can adapt pretrained state-of-the-art models such as AlexNet and VGGNet to decrease the enrollment period.
- DRAMNet can reduce the matching and storage complexity in the system. For example, "strong" PUFs need to store a large number of CRPs in a database for matching, while DRAMNet only needs one set of DRAM power-up values to be embedded into a compact template.

EXPERIMENTAL SETUP AND RESULTS

Experimental Setup

The proposed classifier and two other CNN models (AlexNet[11] and VGGNet[12]) are implemented using the Keras Python library with a TensorFlow backend, which is an open source software library for deep learning launched by

Table 2. Summarized performance results.

Method	Type	Accuracy %		Recall %		Precision %		F-score %	
		SGD	Adam	SGD	Adam	SGD	Adam	SGD	Adam
DRAMNet	Original	91.23	94.35	89.56	94.21	89.29	94.17	88.42	94.19
	Augmented	95.50	98.84	96.69	98.81	96.06	98.73	96.91	98.64
AlexNet	Original	91.89	96.49	91.52	95.39	89.37	96.41	90.43	95.89
	Augmented	96.93	98.69	96.81	98.23	96.66	98.51	96.73	98.36
VGGNet	Original	91.49	95.44	91.07	94.89	88.73	94.73	89.88	94.97
	Augmented	94.72	97.20	94.68	96.95	94.34	96.88	94.50	96.91

Google. For our experiments, 180 different measurements were collected from three different DRAMs based on their power-up values. We specified 60% of the total measurement data (DRAM images) for training DRAMNet and the rest 40% for the testing/evaluation phase. Note that for training data, we ensured that the percentage of DRAM images selected from each particular DRAM was equal. In order to minimize the error rate of the cost function, two different optimization methods, i.e., adaptive moment estimation (Adam) and stochastic gradient descent (SGD) are applied. Since our network is used as a classifier for DRAM authentication with three classes (three DRAMs), SoftMax function is used to predict the probability of each DRAM input.[13]

Evaluation Metrics for Comparison

To evaluate the effective performance of our proposed method, the following four metrics are utilized: accuracy, precision, recall, and F-score. These four metrics are the most frequently used performance indicators for machine learning models. The following equation shows how these metrics are derived:

$$\begin{aligned} Accuracy &= \frac{TP+TN}{TP+TN+FP+FN} \\ Precision &= \frac{TP}{TP+FP} \\ Recall &= \frac{TP}{TP+FN} \\ F_1 - Score &= 2 \times \frac{Precision \times Recall}{Precision+Recall} \end{aligned} \tag{1}$$

where TP, TN, FP, and FN represent the number of true positives, true negatives, false positives, and false negatives, respectively. Moreover, we have also calculated the receiver operation characteristic (ROC) curves. These curves show the tradeoff between false positive rate (FPR) and true positive rate (TPR). FPR refers to the rate at which a classifier incorrectly matches the nonmatching data (outlier) to the target class. TPR refers to the rate that a classifier correctly matches the matching data (target) to the target class.

Classification Results and Discussion

Table 2 presents the summarized performance results of the three CNN models, where DRAMNet refers to our CNN model, and AlexNet and VGGNet refer to other developed CNN architectures. First, the training data were conducted without augmentation. In this case, the DRAMNet CNN model achieved 91.23% average accuracy, 89.56% recall, 89.29% average precision, and 88.42% F-score based on the SGD optimizer. Since our DRAMNet pool is not large enough to achieve the optimal performance, training DRAMNet data can be enlarged by augmenting the DRAM images, which results in higher authentication accuracy. Data augmentation is one of the advantages of applying images as input data into the deep learning technique. We augmented DRAM images by cropping each image in six different ways at the training model. By using this augmentation, our DRAMNet model achieved more than 6% higher accuracy, recall, precision, and F-score. Surprisingly, the authentication performance is increased by applying the Adam optimizer technique for all the models. Based on the results presented in Table 2, the AlexNet CNN model exhibits the best accuracy, recall, and sensitivity precision when we train

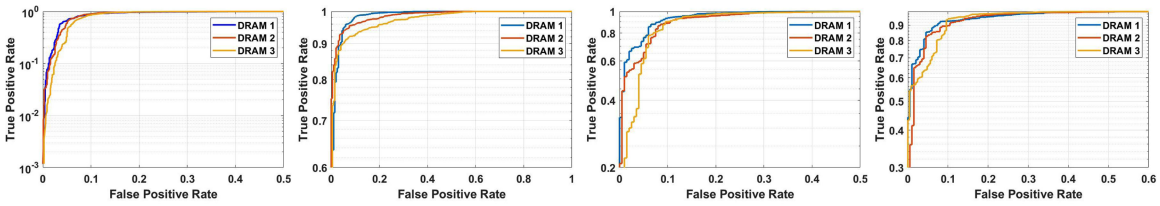

Figure 4. ROC curves of different DRAMs for (a) DRAMNet based on the SGD optimizer, (b) DRAMNet based on the Adam optimizer, (c) VGGNet based on the Adam optimizer, and (d) AlexNet based on the Adam optimizer.

the data based on the SGD optimizer without augmentation.

The discrimination of recall between the DRAMNet method and the highest of the other ones is only 0.06% while the discrimination of precision of the proposed method and the highest of the other ones is 0.1%. In general, we note that data augmentation and the use of the Adam optimizer technique helps all CNN models achieve their highest accuracy, recall, precision, and F-score. In particular, the average accuracy of DRAMNet using the Adam optimizer for original and augmented data is 94.35% versus/and 98.84%, respectively. In addition, the average accuracy of AlexNet and VGGNet is 98.69% and 97.20%, respectively, for augmented data and using the Adam optimizer. Therefore, we observe that the DRAMNet and AlexNet approaches obtain the best classification performance overall. In order to further analyze the performance of the three CNN models, we also study the accuracy of their authentication, using ROC curves. The tradeoffs between TPR and FPR for each CNN model and each of the three DRAMs are shown in the ROC curves presented in Figure 4, and denotes the accuracy of each model.

POTENTIAL APPLICATIONS OF DRAMNET

DRAM is a low-cost high-capacity memory solution that is ideal for embedded hardware. DRAMNet can be applied to any application that uses DRAM and a CNN model. Autonomous vehicles and drones are two examples of how DRAMNet can be applied to developing technologies. The power-up values from various DRAM modules on an autonomous vehicle can be used to identify vehicles without additional resources. The values from a vehicle can be sent to DRAMNet, where it is authenticated by a trusted entity. This type of fast authentication can help with monitoring and communication protocols in autonomous vehicles.

DRAMNet can also be used when applying software updates to autonomous vehicles and drones.[7] Encrypted data from the manufacturer is usually sent to the vehicle, but our proposed method can help validate the correct vehicle to receive the update. Vehicle-to-vehicle communication is also important for an autonomous transportation infrastructure to work correctly. Autonomous vehicles communicate with each other to send warning messages or other information about the current traffic environment. These channels of communication are easy targets for an adversary to attack. DRAMNet could be used as the middle entity to authenticate vehicles on both ends of communication. This ensures that an adversary cannot impersonate another vehicle or try to hijack the communication network.

For the application of unmanned drones, DRAMNet will only allow communication between authenticated devices and users. Service drones that deliver products to a consumer have great potential for this type of authentication. Consumers would have to establish trust by using DRAM images and DRAMNet to authenticate a transaction. However, DRAMNet may be vulnerable to man-in-the-middle or replay attacks where an attacker can manipulate transferred information to the receivers. To overcome this issue, the images that are used for authentication should not be stored after enrollment and communications should employ asymmetric encryption techniques. There is no need to store information after enrollment and this ensures that an attacker cannot retrieve the secret information from memory. As technology develops, medical devices, IoT products, and embedded

systems will have applications where DRAMNet can help with authentication. Overall, DRAMNet allows more control over accessibility of embedded hardware devices.

CONCLUSIONS AND FUTURE WORK

In this article, we have presented a novel authentication method for classifying DRAMs using a deep CNN, "DRAMNet." To evaluate our approach, we utilized data collected from three COTS DRAM modules taken under various environmental conditions. Experimental results have shown that DRAMNet achieved 98.84% accuracy, 98.73% recall, 98.81% precision, and 98.64% F-score. In comparison to the AlexNet and VGGNet models, DRAMNet provides equivalent or better results. We have also shown how the issues with a PUF-based authentication system can be mitigated using our technique. Machine learning attacks and other attacks that create models from CRPs can no longer be used since the entire memory space is needed. We believe that this is a promising direction for future research. Therefore, in the future, we will generate a larger number of DRAM measurements, in order to increase the training pool size of the CNN and improve the accuracy of authentication. We also intend to try these experiments using other types of DRAM modules and characteristics.

REFERENCES

1. B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, 2002, pp. 148–160.
2. F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "DRAM-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 3, pp. 1085–1097, Mar. 2017.
3. A. Schaller *et al.*, "Decay-based DRAM PUFs in commodity devices," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 3, pp. 462–475, May–Jun. 2019.
4. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, 2010, pp. 237–249.
5. M.-D. M. Yu, D. M'Raihi, R. Sowell, and S. Devadas, "Lightweight and secure PUF key storage using limits of machine learning," in *Proc. Cryptographic Hardw. Embedded Syst.*, 2011, pp. 358–373.
6. V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMSEC: Physical unclonable function-based robust and lightweight authentication in the Internet of medical things," *IEEE Trans. Consum. Electron.*, vol. 65, no. 3, pp. 388–397, Aug. 2019.
7. C. Labrado and H. Thapliyal, "Hardware security primitives for vehicles," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 99–103, Nov. 2019.
8. S. K. Kumar, N. Satheesh, A. Mahapatra, S. Sahoo, and K. K. Mahapatra, "Physical unclonable functions for on-chip instrumentation: Enhancing the security of the internal joint test action group network," *IEEE Consum. Electron. Mag.*, vol. 8, no. 4, pp. 62–66, Jul. 2019.
9. T. Addabbo, A. Fort, M. D. Marco, L. Pancioni, and V. Vignoli, "Physically unclonable functions derived from cellular neural networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 12, pp. 3205–3214, Dec. 2013.
10. N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting," *J. Mach. Learn. Res.*, vol. 15, pp. 1929–1958, 2014.
11. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *Proc. 25th Int. Conf. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.
12. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.
13. D. P. Kingma and J. L. Ba, "Adam: A method for stochastic gradient descent," in *Proc. Int. Conf. Learn. Representations*, 2015.
14. G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Proc. Int. Workshop Cryptographic Hardw. Embedded Syst*, 2015, pp. 535–555.
15. J. Shi, Y. Lu, and J. Zhang, "Approximation attacks on strong PUFs," in *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, to be published, doi: 10.1109/TCAD.2019.2962115.

Michael Yue is currently a senior undergraduate student with the Department of Electrical and Computer Engineering as well as the Department of Computer Science Engineering as a double major, Santa Clara University, Santa Clara, CA, USA. He will start the master study in electrical and computer engineering in Fall 2020. His research interests include hardware security and embedded systems. Contact him at myue@scu.edu.

Nima Karimian is currently an Assistant Professor with the Department of Computer Engineering, San Jose State University, San Jose, CA, USA. His research is mainly focused on security and privacy of biometrics, Internet-of-Things and hardware security, and machine learning. He is the recipient of IAPR TC4 Best Paper Award in International Joint Conference on Biometrics (IJCB), 2017.Contact him at nima.karimian@sjsu.edu.

Wei Yan is currently a Postdoctoral Researcher with Washington University in St. Louis, St. Louis, MO, USA. His research interests include FPGA-based digital systems, hardware security, and blockchain. He received the Ph.D. degree from the University of Connecticut, Storrs, CT, USA, in 2018. Contact him at weiyan@wustl.edu.

Nikolaos Athanasios Anagnostopoulos is currently working toward the Ph.D. degree with the Technical University of Darmstadt, Darmstadt, Germany, and is with the University of Passau, Passau, Germany. His research interests include hardware security and embedded systems. Contact him at anagno02@ads.uni-passau.de.

Fatemeh Tehranipoor is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Santa Clara University, Santa Clara, CA, USA. Her research interests include hardware security, Internet-of-Things (IOT) security, and embedded systems. She received "Best Technical Paper Award" in 30th International Conference on VLSI Design (VLSID). She is currently serving as an Associate Editor for IEEE Access and IEEE Consumer Electronics Magazine. Contact her at ftehranipoor@scu.edu.