GAAINet: A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems

Siphesihle P. Sithungu and Elizabeth M. Ehlers
University of Johannesburg, Johannesburg, South Africa
Email: {siphesihles, emehlers}@uj.ac.za

***Abstract*—The expansion of the Internet of Things (IoT) in various industrial sectors (also referred to as the Industrial Internet of Things or IIoT) promises increased economic productivity and quality of life. However, the expansion of IIoT also presents unprecedented security concerns due to increased connectivity between appliances and the cloud. Among the security concerns on IIoT is the threat of intrusions on IIoT networks, resulting in unauthorised access to sensitive data generated by IIoT devices or the compromise of the entire IIoT network. Current work proposes a novel Generative Adversarial Artificial Immune Network (GAAINet) model for intrusion detection in IIoT systems. GAAINet aims to improve the quality of an Artificial Immune Network (AIN)-based classifier by introducing a generator AIN responsible for generating fake intrusion samples from a latent space to fool the classifier (or discriminator) AIN. The adversarial training of the generator and discriminator AINs is expected to improve the intrusion detection capability of the discriminator such that it potentially surpasses traditional training methods that only use preexisting datasets. Current work proposes GAAINet, an immunologically inspired generative adversarial conceptual model, for intrusion detection in IIoT systems.**

***Index Terms*—immunologically inspired computation, generative adversarial models, artificial immune networks, industrial internet of things, industry 4.0**

I. Introduction

Industrial IoT (IIoT) refers to IoT in an industrial application where smart components are embedded into regular (not smart) objects such that those regular objects form part of IoT devices (also referred to as Cyber-Physical Systems (CPS)). Therefore, IIoT is essentially an infrastructure that connects IoT devices to manage them and mine their generated data. The IoT devices in an IIoT infrastructure are referred to as sensors and actuators, and they possess the ability to communicate with other devices. Moreover, the devices themselves require little human intervention to communicate with each other or generate/consume data [1]. IIoT is typically applied to manufacturing, military, agriculture [2], transportation and health services [3].

The general perception is that IIoT could revolutionise factories and other industrial divisions by providing unprecedented cost reductions, operational efficiency, scalability and predictive maintenance. However, these forecasted improvements in the industry also create security concerns. Possible security threats related to IIoT are data loss, workforce injuries, death and cyber-attacks [4]. More specifically, some of the security concerns associated with IIoT are [3]:

- Unauthorised access to information processed by IIoT systems, which may lead to the manipulation or corruption of data.
- Unauthorised access to information being used by an organisation for day-to-day operations and business future decision-making, which may lead to the production of defective products or unwanted changes to production cycles.
- Negative tempering with communication among the IoT devices within the IIoT infrastructure, which may lead to the temporary suspension of production processes or erroneous interactions between the IoT devices.
- Adverse effects on the IIoT infrastructure itself, which may lead to an unwanted transfer of control or changes to the operation of the connected devices.
- The use of the IIoT for malicious actions against an organisation's information system.

Protecting IIoT systems against cyber-attacks is gradually becoming an essential topic of cybersecurity research. One of the research areas aimed at IIoT security is intrusion detection [5]-[9]. In addition, Generative Adversarial Networks (GANs) have been proposed as promising approaches for intrusion detection in IIoT systems [7], [10], [11]. GANs were first introduced by Goodfellow *et al.* in [12] and have been successfully applied to a range of applications such as computer vision [13]-[15], natural language processing [16], [17] and intrusion detection [10], [11], [18]. GANs are usually implemented using artificial neural networks or multilayer perceptrons. The main idea behind GANs is the presence of a discriminator network *D* and a generator network *G*. *G* tries to maximise *D*'s error. In contrast, *D* tries to minimise its error, thereby maximising *G*'s error.

Manuscript received March 11, 2022; revised June 10, 2022.

doi: 10.12720/jait.13.5.456-461

Therefore, *D* and *G* play a MINIMAX game with the value function *V(G,D)* [12].

In the context of a dataset, *G* attempts to generate fake samples which closely resemble samples from the actual dataset. *D* receives samples from both *G* and the existing dataset. The aim is for *D* to be able to tell if a sample comes from the actual dataset (i.e. it is real) or it was generated by *G* (i.e. it is fake) [19]. The algorithm converges when *D* can no longer differentiate between the samples generated by *G* (fake samples) and those from the actual dataset (real).

Therefore, the training process results in a good discriminator because it involves samples from the training set and the generator. The GAN approach is the inspiration behind the proposed GAAINet model, an immunologically inspired approach to training a discriminator Artificial Immune Network (AIN) using a generator AIN.

The reason for applying a generative adversarial approach to AINs is because the concept of antigen recognition, memory retention and self-stabilisation in artificial immune systems makes them a more natural approach to intrusion detection [20].

The rest of the paper is structured as follows. Section II presents the problem statement and similar works from the literature. Section II provides an overview of the GAAINet model. Section IV provides a justification for GAAINet. Finally, Section V concludes the paper and mentions future work.

II. Problem Statement

Industrial IoT (IIoT) infrastructures are a form of Critical Information Infrastructures (CIIs) because they form a critical element of the operations of organisations to which they belong. For example, Cyber-Physical Systems (CPS) can be integrated with IoT devices to create what is referred to as smart industrial systems [21], which are essentially IIoT [22], [23]. Therefore, in terms of the security objectives of Critical Information Infrastructure Protection (CIIP) [24], IIoT infrastructures need to be protected such that:

- Attacks are prevented against IIoT.
- Organisational or national IIoT vulnerabilities are minimised.
- Damages on IIoT due to successful attacks are also minimised.

Therefore, the protection of IIoT should be considered as seriously as the protection of traditional CII. Attacks on IIoT can take on several forms, the most common being (1) attacks on sensors/actuators, (2) attacks on the IIoT gateways, (3) attacks on information being transmitted through the IIoT network, (4) manipulation of remote controller devices, (5) malware injection and (6) denial of service [25]. The current work focuses on intrusion detection approaches in IIoT systems.

There have been works in the literature that proposed possible techniques for intrusion detection in IIoT systems such as distributed agents [8], deep neural networks [9], convolutional neural networks [26] and data streaming [5]. Furthermore, Generative Adversarial Networks (GANs) have also been proposed for intrusion detection in IIoT.

The following subsection presents a literature review of methods that used GANs for intrusion detection in IIoT, among other AIS-based methods.

A. Similar Works

1) Generative adversarial network-based methods for intrusion detection in IIoT

This section covers works that exist in the literature that proposed the use of GANs for intrusion detection in IIoT systems (more specifically, Cyber-Physical Systems (CPSs) [10]. The list may not be exhaustive, but it presents the most relevant works for this paper.

De Araujo-Filho *et al.* [7] proposed a system referred to as FID-G, an unsupervised intrusion system for CPSs that utilises GANs and uses fog computing. The purpose of making FID-GAN fog-based was to bring computational resources closer to the end nodes to achieve low latency. FID-GAN made use of a reconstruction loss (computed based on reconstructed data samples from the latent space) to improve detection rates. Furthermore, an encoder was used to accelerate the process of computing the reconstruction loss since the problem domain required low latency when it comes to detection. As a result, FID-GAN produced promising detection rates and latency [7].

Taheri *et al.* [27] proposed the FED-IIoT architecture for detecting Android malware applications in IIoT systems based on federated learning. The architecture consisted of two segments: (1) a participant side where a GAN and a Federated GAN (FedGAN) were used to generate dynamic poisoning attacks, and (2) a server-side which monitored the global model and provided a collaborative training model for detecting malware. The server side made use of an A3GAN (avoiding anomaly in aggregation using a GAN). The system was evaluated using three existing IoT datasets, and it was noted in the paper that the system achieved approximately 8% higher accuracy than existing state-of-the-art methods [27].

Hassan *et al.* [11] proposed a downsampler-encoder-based cooperative data generator (trained using an adaptive algorithm) to improve the generation of attack data samples for IIoT environments. The proposed data generator was based on the fact that standard GAN-based generators generate adversarial examples based on randomly sampled noise. The use of randomly sampled noise resulted in a distribution that differed significantly from the actual distribution of data in IIoT networks, which led to decreased robustness against attacks. A deep neural network was used as a downsampler (i.e., downsampling high-dimensional input to lower dimensions). Another deep neural network was used to classify the downsampled (encoded) features. It was shown that the method proposed in [11] outperformed conventional deep neural network-based techniques and other machine learning-based techniques, such as support vector machines [11]. Although this method did not use a GAN, it was explored here because it aimed to improve the shortcomings of GAN-based data generation in IIoT.

2) Artificial immune system-based methods for intrusion detection in IIoT

Apart from methods based on adversarial data generation (as explored in Section II.*A.1)*), several artificial immune system-based methods have also been proposed as possible approaches for achieving intrusion detection in IIoT systems. Although no published papers were found in the literature presenting AIS approaches in IIoT (at the time of writing of this paper), this section explores works that proposed AIS approaches in IoT.

Aldhaheri *et al*. [28] proposed a network-based method that uses an AIS called DeepDCA (Deep Learning and Dendritic Cell Algorithm) for intrusion detection in IoT. DeepDCA used the dendritic Cell Algorithm (DCA) and a Self-Normalising Neural Network (SNN) to classify intrusions and minimise the generation of false alarms. The method was tested on the IoT-Bot dataset, where the SNN's task was to perform signal categorisation and the DCA classification. As a result, DeepDCA achieved 98.73% accuracy and a low false-positive rate and outperformed several state-of-the-art techniques [28].

Brown and Anwar [29] proposed Blacksite, a human-in-the-loop method that used an AIS for adaptive real-time intrusion detection in IoT networks. Blacksite combined human intelligence, AIS, and a Deep Neural Network (DNN) validation model. The AIS component used a T-Cell inspired algorithm to generate detectors. The DNN was used to validate if specific network traffic was indeed suspicious. The role of the human-in-the-loop was to confirm whether flows flagged by the DNN were suspicious based on training and experience. Preliminary results showed that the proposed DNN-based approach achieved an accuracy of 99.74%.

There is not a relatively large body of work in the literature based on GANs for intrusion detection in IIoT. Moreover, the works in the literature are relatively recent, which is reason to suggest that this is an ongoing area of research. The problem background and a literature study of similar works have been addressed, and the following section presents the proposed GAAINet model.

III. GAAINet: Model Overview

This section presents an overview of GAAINet. It is important to note that GAAINet is still a conceptual model, meaning it has not been physically implemented and tested for applicability. Therefore, this paper aims to propose GAAINet as a conceptual model. The model's implementation results are expected to be published in future work. A proof-of-concept prototype will be constructed and tested on various intrusion detection datasets to explore how GAAINet performs when applied to an IIoT dataset. As such, the proposed study focuses on the invention of a novel immunologically inspired generative adversarial model for intrusion detection in IIoT systems.

GAAINet is inspired by the successful application of GANs in various tasks based on intrusion detection, computer vision and natural language processing. Other generative models exist, such as Restricted Boltzmann Machines (RBMs) [30], Deep Boltzmann Machines (DBMs) [31] and Deep Belief Networks (DBNs) [32]. However, the advantage provided by GANs is that there is no need to utilise approximate inference, Markov chains or Monte Carlo methods during training or generation processes because backpropagation can be used to train the entire GAN [10], [12].

The structure of a typical GAN can be seen in Fig. 1. The generator model uses random noise to generate examples/samples from a latent space for the discriminator model to classify the examples as either real or fake.

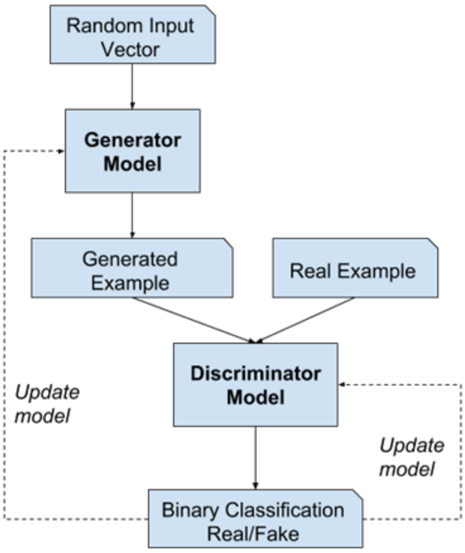

Figure 1. A traditional GAN architecture [33].

Typically, the generator model does not know what the examples from the actual dataset look like, and the goal is for it to learn a distribution from the latent space. For the generator to improve in generating fake examples that seem real, a loss function is used to update its weights accordingly. The discriminator also has a loss function, which updates the discriminator's weights. The discriminator receives examples from both the generator and the actual dataset. Therefore, the output from the discriminator is used to update the parameters of both the generator and discriminator.

Current work proposes the realisation of a generative adversarial model based on Artificial Immune Networks (AINs). AINs are part of the AIS family of algorithms and are inspired by the Immune Network Theory (INT) initially proposed by Niels Jerne [34].

An immune network (or immune network model) typically aims to represent networks of antibodies that interact with each other without the presence of antigens and are also known as idiotypic networks [35]. The initial state of an immune network can be thought of as a set of interacting antibodies in the form of a graph data structure. From a graph theory perspective, the affinities between the antibodies can be considered as connection weights.

In order to cause changes in the network (i.e., the connection weights between nodes), examples/data samples are fed into the network, where each sample is thought of as an antigen entering the immune network and stimulating the antibodies in the network. Thus, iteratively providing data samples to the network results in a complex graph of interacting antibodies. The process results in a graph representing an abstract representation of the dataset. Fig. 2 illustrates the process.

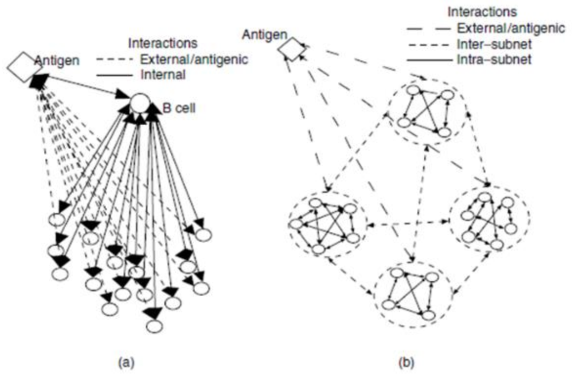

Figure 2. An AIN is represented as a graph data structure [35].

As shown in Fig. 2, presenting data samples (i.e. antigens) to the AIN results in a change in the structure of the AIN and the connection strength between the nodes of the AIN. Therefore, AINs can be used for unsupervised learning, where the final structure of the network is an illustration/representation of the different classes in the training dataset.

Furthermore, the final structure of the AIN (after training) can be used to categorise new samples into classes based on what was learned in the dataset, which means that AINs can theoretically be used to perform multi-class classification.

For example, suppose that an AIN is used as a classifier as described above. This paper proposes that a generator AIN responsible for generating fake data samples can be constructed such that it learns an abstract representation of part of a latent space, which would allow it to generate examples potentially good enough to "fool" the discriminator.

1) Training the discriminator and generator AINs: A semi-supervised learning approach

There must be an approach for training the discriminator and the generator AINs to realise a properly functioning model. The discriminator AIN can be trained using an existing dataset representing actual intrusion samples. After the training set has been fed to the discriminator, it should have discovered patterns in the dataset used to form a *model* of what is *real*. Therefore, the process of training the discriminator from the training set is entirely unsupervised. Fig. 3 illustrates the process.

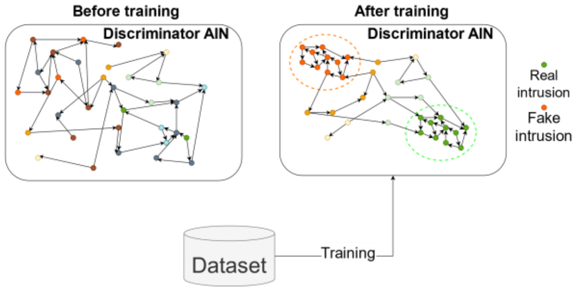

Figure 3. The discriminator AIN during training.

After training the discriminator using the training set, the next step should be to train the generator. While the generator is being trained, the discriminator's network structure does not change. When a new example is fed into the discriminator, it should only output a class prediction and not update its state (like it would during its training phase). Therefore, the generator AIN should produce examples for the discriminator to classify, and the discriminator should only indicate if the examples are real or fake (please see Fig. 4).

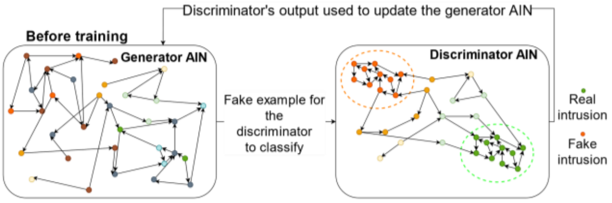
Discriminator's output used to update the generator AIN
Before training
Generator AIN
Fake example for the discriminator to classify
Discriminator AIN
Real intrusion
Fake intrusion

Figure 4. The generator AIN is trained using the discriminator AIN's output/predictions.

The output of the discriminator must be used as feedback for the generator, which it must use to update itself so that it improves the *quality* of the examples it generates in the future. Therefore, the process of training the generator is semi-supervised. Fig. 5 illustrates the process.

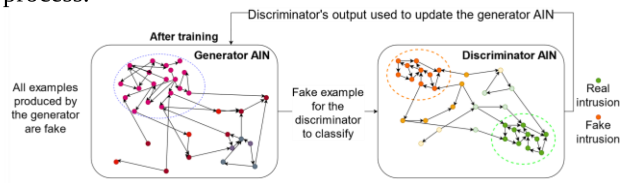
Discriminator's output used to update the generator AIN
After training
Generator AIN
All examples produced by the generator are fake
Fake example for the discriminator to classify
Discriminator AIN
Real intrusion
Fake intrusion

Figure 5. The generator AIN after training.

It is important to note that, since the generator never has access to the dataset containing real examples, it *always* generates fake samples. The generator aims to create fake samples that can *fool* the discriminator into "thinking" that they are real. Suppose the generator reaches a point where it can fool the discriminator. That would mean it is time for the discriminator to start updating its network to learn to detect the generator's fakes more efficiently. The discriminator's output must now be fed back to the itself to update its network structure and connection weights (please see Fig. 6). Therefore, updating the discriminator after the generator becomes good enough is also semi-supervised.

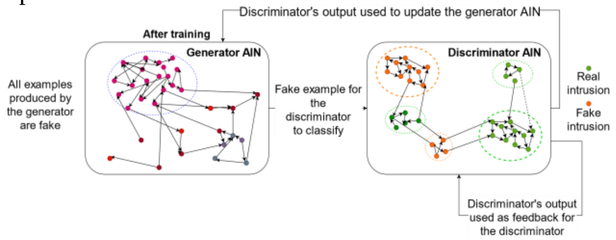
Discriminator's output used to update the generator AIN
After training
Generator AIN
All examples produced by the generator are fake
Fake example for the discriminator to classify
Discriminator AIN
Real intrusion
Fake intrusion
Discriminator's output used as feedback for the discriminator

Figure 6. The discriminator's internal state is updated to improve its detection ability.

Establishing a feedback loop for the discriminator AIN is expected to ensure that the AIN remains adaptive even after training. Moreover, the generator AIN is expected to improve continuously as the discriminator improves. The generator AIN represents an attacker for the discriminator to continuously test itself against even without intrusions in the IIoT network. Furthermore, since IIoT systems are highly dynamic, a model that continuously adapts itself after training should result in a robust intrusion detection solution.

IV. GAAINet: Justification

Section III provided an overview description of GAAINet. However, a description of the model does not necessarily justify why it should be implemented in practice. The purpose of this section is to provide a justification for proposing GAAINet, more especially for intrusion detection in IIoT systems.

The first justification for proposing GAAINet is that IIoT systems are highly dynamic. Therefore, models that are only trained offline and are not adaptive to change can be a disadvantage in IIoT systems since the nature of attacks is also dynamic. GAAINet makes use of artificial immune networks, which are adaptive, and this is expected to compensate for the dynamic nature of IIoT systems as well as attacks on them. Furthermore, it was noted that after the generator AIN has been trained enough to fool the discriminator AIN, the discriminator AIN can be updated online so that it forms new representations of what is real and fake. This feature of GAAINet makes it worth proposing for intrusion detection in IIoT systems.

Secondly, intrusion detection systems in IIoT are still an active area of research. As noted in the problem background (Section II), research on intrusion detection that focuses explicitly on IIoT has not saturated, which means there is still room for contributions. Furthermore, a significantly small amount of work is based on Artificial Immune Systems (AIS) for intrusion detection in IIoT (noted in the literature review). AINs (a kind of AIS) are adaptive and, therefore, feasible to intrusion detection in dynamic environments.

Thirdly, there is an increasing availability of IIoT datasets in the literature, which means it should gradually become easier to create benchmarks for comparing IIoT intrusion detection systems. In the context of GAAINet, this means that the model can be trained on different IIoT datasets to provide more insights into its applicability and robustness. GAAINet is still a conceptual model whose implementation results must be reported in future work.

Finally, GAAINet can be applied to other use cases apart from intrusion detection. GAAINet can be applied to other use cases requiring adaptive models trained in a semi-supervised approach, such as games, image/text generation, robotics, and specific tasks requiring machine learning.

V. Conclusion and Future Work

This paper presented GAAINet, an immunologically inspired generative adversarial model for intrusion detection in IIoT systems. First, a description of IIoT and GANs was provided, followed by the problem background. The problem background emphasised the importance of protecting IIoT since it also forms part of organisational/national Critical Information Infrastructure (CII).

It was noted that the importance of safeguarding IIoT should be treated the same as with CII. The literature review was divided into (1) generative adversarial networks for intrusion detection in IIoT and (2) artificial immune systems for intrusion detection in IIoT. It was also noted that many applications of AISs for intrusion detection in the literature were based on IoT and not IIoT.

The literature review was followed by an overview of GAAINet, which first described GANs and AINs in detail. It was noted that training must take place in two phases. The first training phase must focus on training the discriminator AIN in an unsupervised learning style to learn its representation of the dataset. The second training phase must focus on training the generator using outputs provided by the discriminator until the generator becomes good at fooling the discriminator.

After training, the discriminator must be continuously updated using a feedback mechanism. Whenever the discriminator makes incorrect predictions (classifying fake samples as real), the discriminator's output must be fed back into the discriminator. Section IV provided four justifications for proposing of GAAINet. Each of the justifications specified how the architecture, semi-supervised learning approach and adaptive nature of GAAINet make it a model worth considering in the context of IIoT and other relevant problem domains. Future work aims to implement a GAAINet proof-of-concept prototype that must be tested for applicability as an intrusion detection system for IIoT.

Conflict of Interest

This is a declaration that the submitted work was not carried out with a conflict of interest.

Author Contributions

This paper is part of Mr. SP Sithungu's PhD research, and Prof. E. M. Ehlers is the PhD study supervisor. As such, SP Sithungu's contribution to this specific paper was conducting the research, formalising the proposed model and writing the paper. E. M. Ehlers' contribution was ensuring that the paper's contents are up to the required standard, guiding the research and providing expert advice regarding the proposed model.

References

[1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, pp. 1-12, 2018.

[2] N. Sharma, "Evolution of IoT to IIoT: Applications & challenges," *SSRN Electronic Journal*, Jul. 2020.

[3] S. Figueroa-Lorenzo, J. Añorga, and S. Arrizabalaga, "A survey of IIoT protocols: A measure of vulnerability risk analysis based on CVSS," *ACM Comput. Surv.*, vol. 53, no. 2, Apr. 2020.

[4] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models," in *Proc. IEEE Wireless Communications and Networking Conference Workshops,* 2018, pp. 173-178.

[5] I. Butun, M. Almgren, V. Gulisano, and M. Papatriantafilou, "Intrusion detection in industrial networks via data streaming," in *Industrial IoT : Challenges, Design Principles, Applications, and Security*, I. Butun, Ed., Cham: Springer International Publishing, 2020, pp. 213-238.

[6] S. L. P. Yasakethu and J. Jiang, "Intrusion detection via machine learning for SCADA system protection," in *Proc. 1st International Symposium for ICS & SCADA Cyber Security Research 2013*, 2013, pp. 101-105.

[7] P. D. Araujo-Filho, G. Kaddoum, D. R. Campelo, A. Gondim Santos, D. Macêdo, and C. Zanchettin, "Intrusion detection for cyber-physical systems using generative adversarial networks in fog environment," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6247-6256, 2021.

[8] M. Niedermaier, M. Striegel, F. Sauer, D. Merli, and G. Sigl, "Efficient intrusion detection on low-performance industrial iot edge node devices," arXiv preprint arXiv:1908.03964, 2019.

[9] S. Latif, Z. Idrees, Z. Zou, and J. Ahmad, "DRaNN: A deep random neural network model for intrusion detection in industrial IoT," in *Proc. International Conference on UK-China Emerging Technologies*, 2020, pp. 1-4.

[10] V. Belenko, V. Chernenko, M. Kalinin, and V. Krundyshev, "Evaluation of GAN applicability for intrusion detection in self-organising networks of cyber physical systems," in *Proc. International Russian Automation Conference*, 2018, pp. 1-7.

[11] M. M. Hassan, M. R. Hassan, S. Huda, and V. H. C. D. Albuquerque, "A robust deep learning enabled trust-boundary protection for adversarial industrial IoT environment," *IEEE Internet of Things Journal*, p. 1, 2020.

[12] I. J. Goodfellow, *et al.*, "Generative adversarial networks," *Advances in Neural Information Processing Systems*, vol. 27, 2014.

[13] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, "Improved techniques for training gans," arXiv preprint arXiv:1606.03498, 2016.

[14] C. Li, K. Xu, J. Zhu, and B. Zhang, "Triple generative adversarial nets," arXiv preprint arXiv:1703.02291, 2017.

[15] T. Xu, *et al.*, "Attngan: Fine-Grained text to image generation with attentional generative adversarial networks," in *Proc. IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 1316-1324.

[16] Y. Saito, S. Takamichi, and H. Saruwatari, "Text-to-Speech synthesis using STFT spectra based on low-/multi-resolution generative adversarial networks," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, 2018, pp. 5299-5303.

[17] C. D. M. D'Autume, M. Rosca, J. Rae, and S. Mohamed, "Training language gans from scratch," arXiv preprint arXiv:1905.09922, 2019.

[18] M. Usama, M. Asim, S. Latif, and J. Qadir, "Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems," in *Proc. 15th International Wireless Communications & Mobile Computing Conference*, 2019, pp. 78-83.

[19] A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, "Generative adversarial networks: An overview," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 53-65, 2018.

[20] I. Dutt, S. Borah, and I. Maitra, "Intrusion detection system using artificial immune system," *International Journal of Computer Applications*, vol. 144, no. 12, 2016.

[21] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375-1384, 2016.

[22] G. Hatzivasilis, K. Fysarakis, O. Soultatos, I. Askoxylakis, I. Papaefstathiou, and G. Demetriou, "The industrial internet of things as an enabler for a circular economy Hy-LP: A novel IIoT protocol, evaluated on a wind park's SDN/NFV-enabled 5G industrial network," *Computer Communications*, vol. 119, pp. 127-137, 2018.

[23] D. Zhang, C. C. Chan, and G. Y. Zhou, "Enabling Industrial Internet of Things (IIoT) towards an emerging smart energy system," *Global Energy Interconnection*, vol. 1, no. 1, pp. 39-47, 2018.

[24] E. Nickolov, "Critical information infrastructure protection: Analysis, evaluation and expectations," *An International Journal*, vol. 17, pp. 105-119, Apr. 2005.

[25] V. Sklyar and V. Kharchenko, "ENISA documents in cybersecurity assurance for Industry 4.0: IIoT threats and attacks scenarios," in *Proc. 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 2019, pp. 1046-1049.

[26] Y. Li, *et al.*, "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," *Measurement*, vol. 154, p. 107450, 2020.

[27] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "FED-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Transactions on Industrial Informatics*, p. 1, 2020.

[28] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani, and A. Al-Barakati, "DeepDCA: Novel network-based detection of IoT attacks using artificial immune system," *Applied Sciences*, vol. 10, no. 6, 2020.

[29] J. Brown and M. Anwar, "Blacksite: Human-in-the-Loop artificial immune system for intrusion detection in internet of things," *Human-Intelligent Systems Integration*, vol. 3, no. 1, pp. 55-67, 2021.

[30] H. Zhang, S. Zhang, K. Li, and D. N. Metaxas, "Robust shape prior modeling based on Gaussian-Bernoulli restricted Boltzmann Machine," in *Proc. IEEE 11th International Symposium on Biomedical Imaging*, 2014, pp. 270-273.

[31] R. Salakhutdinov and H. Larochelle, "Efficient learning of deep Boltzmann machines," in *Proc. the Thirteenth International Conference on Artificial Intelligence and Statistics*, 2010, pp. 693-700.

[32] F. Khalid and M. I. Fanany, "Combining normal sparse into discriminative deep belief networks," in *Proc. International Conference on Advanced Computer Science and Information Systems*, 2016, pp. 373-378.

[33] J. Brownlee, "A gentle introduction to Generative Adversarial Networks (GANs)," *Machine Learning Mastery*, Jul. 19, 2019.

[34] M. Rucco, F. Castiglione, E. Merelli, and M. Pettini, "Characterisation of the idiotypic immune network through persistent entropy," in *Proceedings of ECCS 2014*, Springer, 2016, pp. 117-128.

[35] D. Dasgupta and F. Nino, *Immunological Computation: Theory and Applications*, CRC Press, 2008.

Siphesihle P. Sithungu was born in the east of Johannesburg, South Africa in the year 1993 and holds the following qualifications: BSc computer science and informatics, University of Johannesburg, South Africa (obtained 2017); BSc Hons in computer science, University of Johannesburg (obtained 2018); MSc in computer science, University of Johannesburg (obtained 2020).

He is currently employed as a lecturer at the University of Johannesburg, South Africa on a full-time basis and his research interests are multi-agent systems, machine learning and nature inspired artificial intelligence.

Mr. Sithungu is a member of the technical committee for the International Conference on Computational Intelligence and Intelligent Systems.

Elizabeth M. Ehlers started her research career in the discipline of formal languages and automata theory. Prof Ehlers holds a PhD. in Computer Science awarded by the former Rand Afrikaans University with a thesis titled: A Hierarchy of Random Grammars and Automata.

Currently her main research interests are agent architectures and interesting applications thereof. This includes multi-agent systems, Artificial Intelligence and specifically AI applications.

Prof. Ehlers has been full professor in the Academy of Computer Science and Software Engineering at the University of Johannesburg since 1992. She was appointed Head of Department of the Academy of Computer Science and Software Engineering in 2007.