Generative Adversarial Networks for Anomaly Detection in ICS

UNDERGRADUATE THESIS

Submitted in partial fulfillment of the requirements of
BITS F421T Thesis

By

Surya GARIKIPATI
ID No. 2019AATS1221H

Under the supervision of:

Dr. Aditya P. MATHUR
&
Dr. Joyjit MUKHERJEE

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, HYDERABAD CAMPUS
December 2022

Certificate

This is to certify that the thesis entitled, "*Generative Adversarial Networks for Anomaly Detection in ICS*" and submitted by Surya GARIKIPATI ID No. 2019AATS1221H in partial fulfillment of the requirements of BITS F421T Thesis embodies the work done by him under my supervision.

Supervisor	*Co-Supervisor*
Dr. Aditya P. MATHUR	Dr. Joyjit MUKHERJEE
Professor,	Assistant Professor,
Singapore University of Technology and Design	BITS-Pilani Hyderabad Campus
Date:	Date:

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE PILANI, HYDERABAD CAMPUS

Abstract

Bachelor of Engineering Electronics and Communication Engineering

Generative Adversarial Networks for Anomaly Detection in ICS

by Surya GARIKIPATI

Anomaly Detection is a significant problem that has been researched for many years now. As technology has developed and with an increase in more complex problems, traditional methods for anomaly detection have been performing more poorly. In this report, we attempt to bring forth a more recent neural network model called general adversarial networks (GANs). GANs can simulate the intricate, high-dimensional distributions of real-world data, hence they can represent a possible solution to this problem. GANs have been exceptional at correctly identifying and detecting anomalies in different data sets. In this paper, we run GANs on the Secure Water Treatment (SWaT) and the Water Distribution (WADI) industrial control system (ICS) testbed dataset. We compare various popular GANs against each other and to traditional anomaly detection models. These approaches still have a lot of potential for improvement in terms of computing cost and anomaly detection accuracy.

Acknowledgements

I would like to thank Prof. Aditya P. Mathur and PhD Candidate Mr. Gauthama Raman MR for guiding me through this project and providing prompt and effective feedback and critique on my work wherever necessary. I would further like to thank Dr. Joyjit Mukherjee for Co-Supervising my undergraduate thesis and providing guidance and spending his time to review my work. I would also like to thank all the examiners who are grading my report for taking their time to review the work that I have done till now. Last but not least, I would like to thank my parents for providing me the frame work and constant motivation to work hard and try my best to achieve the outcomes of this research project.

Contents

Generative Adversarial Networks for Anomaly Detection in ICS

Introduction and Motivation

Anomaly Detection is one of the crucial problems across a wide range of domains including manufacturing, medical imaging, and cyber-security. Data can be complicated and multidimensional, therefore anomaly detection techniques must simulate the distribution of typical data. An important issue in several study fields is anomaly detection. Identifying hidden data and accurately classifying it as anomalous is a difficult problem that has been addressed in a variety of ways over time. An electronic control system and related apparatus used for industrial process control are known as an industrial control system (ICS). Some popular examples of industrial control systems are power plants, water treatment, and distribution plants, autonomous vehicles, etc. One of the possible risks to ICSs that causes the most worry is cyberattacks.

Traditional methods of machine learning such as linear model-based methods, distance-based methods, and support vector machines, among others have always been the norm for anomaly detection. These models although efficient and great models often struggle in detecting anomalies in time series in which the data is more complex and random. Particularly, it is difficult to spot anomalies in time-series data since both the causation and the order of observations along the time axis must be taken into account. Since time-series data has been extensively researched in academic fields like economics, meteorology, and medicine, it is now a crucial component of analysis in the majority of practical applications. The term ”time-series analysis” refers to a variety of tasks that attempt to extract meaningful knowledge from time-ordered data; the knowledge so obtained may be used to both diagnose and forecast previous behavior. Anomalies are often uncommon, most supervised approaches don't use enough relevant normal data or tagged anomaly classes to learn from. The majority of unsupervised algorithms now in use are constructed via linear projection and transformation, yet the multivariate time series of complex ICSs frequently exhibit nonlinearity in their hidden underlying correlations.

When compared to conventional machine learning algorithms, deep learning, a branch of machine learning algorithms that draws inspiration from the structure and operation of the brain, has improved anomaly detection. These methods were created to handle multivariate and high-dimensional data. This removes the difficulties of separately modeling anomalies for each variable and averaging the findings, making it simple to integrate data from several sources. Deep learning techniques are also well suited to simultaneously modeling the interactions between several factors with regard to a specific task and need less fine-tuning to provide effective results. Performance is another benefit since it allows for the modeling of intricate, nonlinear connections within the data, which is useful for the task of anomaly identification. These qualities set them apart from earlier methods and made them a desirable option for time-series analysis.

In recent years, a type of deep learning method called general adversarial networks has been introduced that helped improve anomaly detection. The success of general adversarial networks in anomaly detection has motivated researchers to continue their work on general adversarial networks in anomaly detection. Even though GAN has demonstrated astounding success in image processing tasks like creating realistic-looking pictures, there has only been a small amount of effort done so far to apply the GAN framework to time-series data. However, in these early studies, the GAN framework has been shown to be successful in creating time series sequences, whether to create polyphonic music using recurrent neural networks as the generator and discriminator or to create real-valued medical time series using a conditional version of recurrent GAN. In recent years, many new types of general adversarial network models have been introduced and have performed incredibly compared to traditional machine learning models and neural networks.

In this thesis, we bring forth GAN-based anomaly detection that is efficient during testing in addition to being effective. Reviewing cutting-edge generative adversarial network-based anomaly detection techniques for time-series data is the aim of this paper. We employ a family of GANs that simultaneously train an encoder network, enabling more rapid and effective inference during testing. The GAN-trained discriminator, in contrast to conventional classification techniques, learns to distinguish false data from genuine data in an unsupervised manner, making it an appealing unsupervised machine learning methodology for anomaly detection. We look closely at their definition of interrelationships between variables, how they understand temporal context, and how they spot abnormalities in multivariate time series. We run these well-developed GAN models on the SWaT and WADI datasets and compare the efficiency and effectiveness of these models. We hope to further improve these models' efficiency to receive more phenomenal results in GAN-based anomaly detection.

Related Works

Anomaly detection has always been an extensively studied area of research. Here, we provide a succinct summary and direct you to these evaluations for a more thorough discussion. Distance-based approaches, which use distances between nearest neighbors or clusters in the data to determine if data is anomalous, are a prominent class of traditional anomaly detection methods. Such techniques rely on the data being mapped to a suitable distance measure. One-class SVMs, which learn a classification border around the normal data, are one example of a one-class classification strategy that is often utilized. If an example is anomalous, the third class of approaches leverages fidelity of reconstruction to make the determination. Such techniques include principal component analysis and its variations.

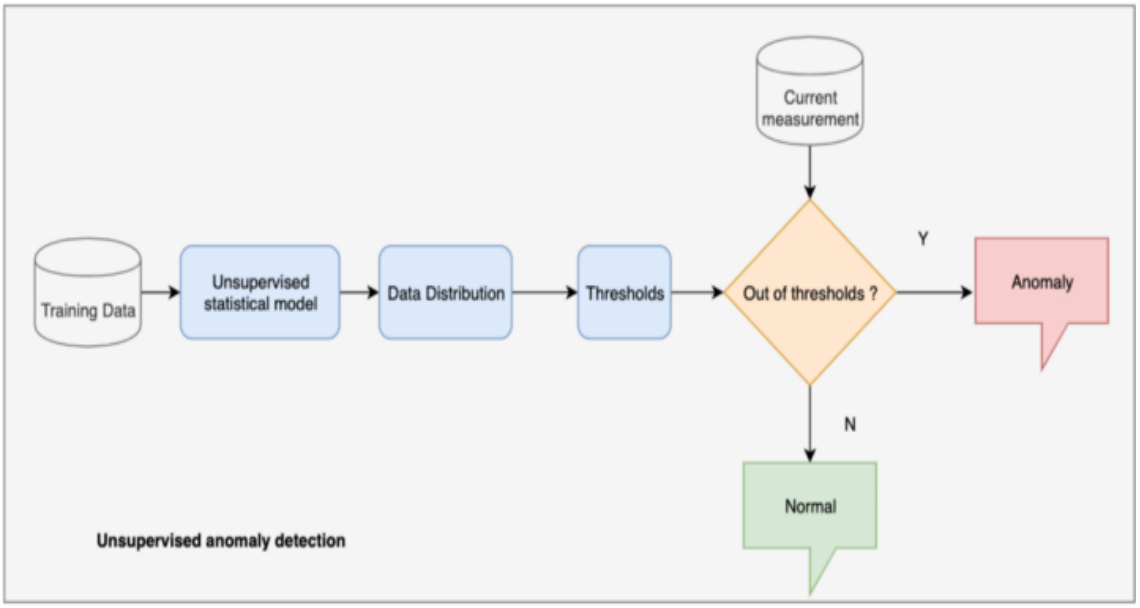

FIGURE .1: Figure contains a rough idea of how anomaly detection works. Credits: https://medium.com/safetycultureengineering/approaches-to-anomaly-detection-20de4983d23/

Deep neural networks have been employed in more recent research, and neural networks have long been used for anomaly identification. The use of autoencoders and variational autoencoders allows for the training of models to reconstruct normal data before identifying samples with significant reconstruction errors as anomalies. Deep auto-encoding Gaussian mixture models and energy-based models have also been investigated expressly for this function. These techniques use auto-encoders or comparable models to simulate the distribution of the data and then create a statistical anomaly criterion based on the energies or mixes of Gaussians.

GANs have been used in the context of medical imaging on retinal scans to detect anomalies. The methods suggested, however, call for a test-time inference approach where latent variables z is recovered using stochastic gradient descent for each test case. The minimax loss function is used to train GAN in the GAN-based anomaly detection approaches, where the generator seeks to produce samples that overlap with the data distribution. The discriminator probability score was found to be unsuccessful when using the standard GAN loss function, and we assume that this is because the discriminator was not explicitly trained to fence the edge of the data distribution. Since each gradient computation necessitates backpropagation across the generator network, this inference technique is computationally costly.

General Adversarial Networks

Generative models can be trained using general adversarial networks (GANs) as an alternative framework to circumvent the challenge of approximating several intractable probabilistic calculations. One type of model that has been utilized well to simulate complicated and high dimensional distributions is generative adversarial networks (GANs). GANs consist of a generator G and a discriminator D. The Generator creates phony data samples in an effort to deceive the Discriminator. On the other hand, the Discriminator tries to tell the difference between genuine and fraudulent samples. Both the Generator and the Discriminator are neural networks, and throughout the training phase, they compete with one another. The procedures are repeated multiple times, and each time, the Generator and Discriminator become better at what they are doing. This can be better visualized in the diagram below.

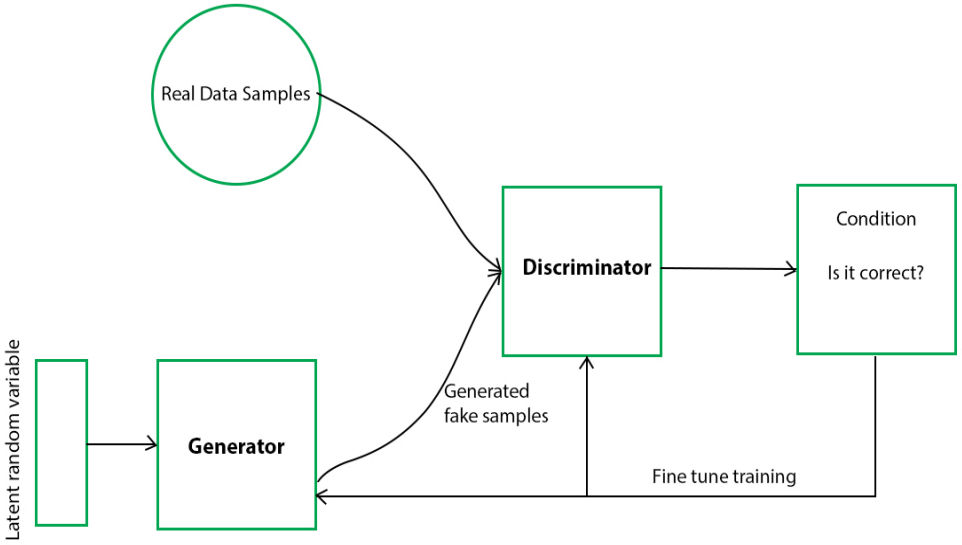

FIGURE .2: Figure contains a rough diagram of how a General Adversarial Network works. Credits: https://www.geeksforgeeks.org/generative-adversarial-network-gan/

The generative model, which is trained to try to increase the likelihood that the Discriminator would make a mistake, captures the distribution of data. On the other hand, the Discriminator is based on a model that calculates the likelihood that the sample it received came from the training data and not the generator. The Discriminator is seeking to reduce its reward V(D, G) in the minimax game that the GANs are designed as, while the Generator is aiming to maximize its loss by minimizing the Discriminator's reward. This can be seen with the mathematical formula below:

$$\min_G \max_D V(D,G)$$

$$V(D,G) = \mathbb{E}_{x \sim p_{data}(x)}[\log D(x)] + \mathbb{E}_{z \sim p_z(z)}[\log(1 - D(G(z))]$$

In this mathematical formula, the Discriminator and Generator are represented by D and G respectively. Pdata(x) is the distribution of real data and P(z) is the distribution of the generator. X and Z are samples from Pdata(x) and P(z) respectively. D(x) is the discriminator network and G(z) is the generator network.

Training a GAN has two parts. First, while the Generator is not in use, the discriminator is being taught. The network is only forward propagated during this phase; no backpropagation is carried out. The Discriminator is tested to determine if it can accurately identify them as real after being trained on actual data for n epochs. Additionally, the Discriminator is trained on the fictitious data produced by the Generator at this phase to determine if it can correctly identify them as such. And then while the Discriminator is not in use, the Generator is being taught. After the Discriminator has been trained using the Generator's fabricated data, we may utilize the predictions to train the Generator and improve from the Discriminator's prior state.

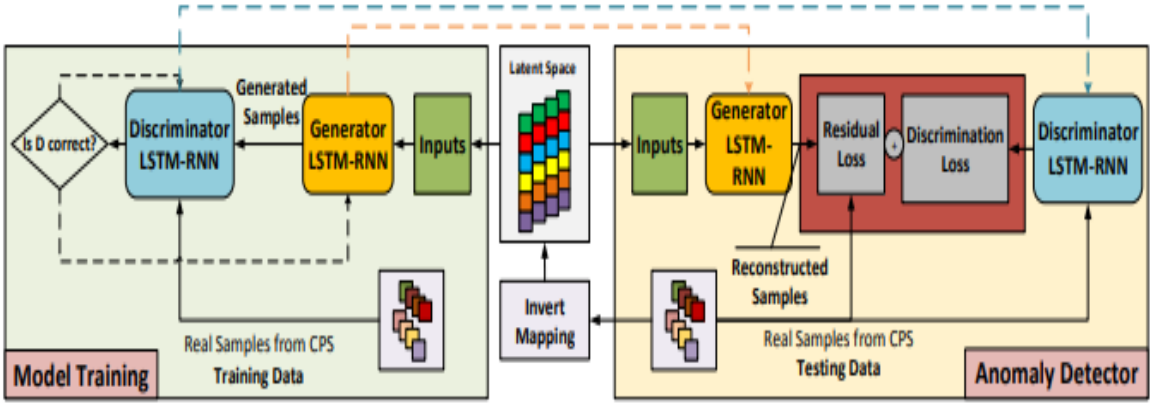

FIGURE .3: Figure is how GAN-AD an LTSM-RNN based general adversarial network functions in a multivariate time series Credits: "Anomaly Detection with Generative Adversarial Networks for Multivariate Time Series" published by Dan Li, Dacheng Chen, Jonathan Goh, and See-Kiong Ng,

Multi-variate Time Series Anomaly Detection

Time series are collections of data that are constantly recorded throughout time. Univariate and multivariate time series are two major categories for time series data. Only one variable changes over time in a univariate time series. A Multivariate time series is when multiple variables vary over time. It might be difficult to find anomalies in multivariate time series data. Diagnostics for fault isolation are made possible by effective multivariate anomaly detection. It is demonstrated that the RNN and LSTM-based approaches 3 are effective in locating interpretable abnormalities in multivariate time series datasets. Lack of established patterns in which an anomaly may be characterized, input data noise that substantially impairs algorithm performance, and rising computational complexity as time series data lengthens are of some of the many difficulties in detecting anomalies in time series data.

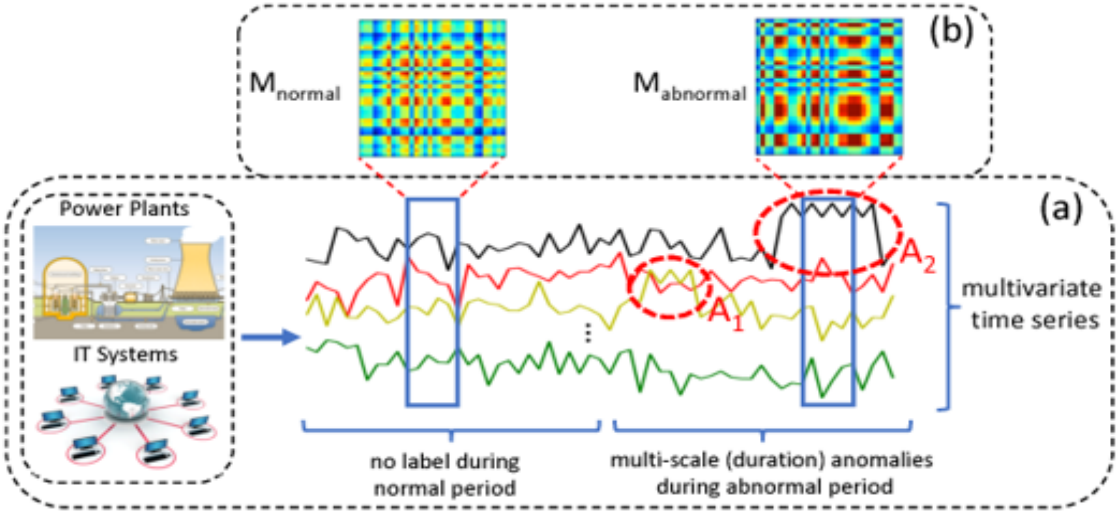

FIGURE .4: Figure is how GAN-AD an LTSM-RNN based general adversarial network functions in a multivariate time series Credits: "A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series Data" published by Chuxu Zhang

GANs on Anomaly Detection

Given that typical GANs only enable efficient sampling, there are a number of ways to modify them to identify anomalies. As an illustration, one may utilize sampling to assess whether a data point x is an outlier and estimate its likelihood. While using a GAN for sampling is effective, good likelihood estimate frequently calls for a high number of samples, making the likelihood calculation computationally costly. Another strategy is to "invert" the generator to use stochastic gradient descent to identify latent variables z that reduce reconstruction error or other related goals. Because each gradient computation necessitates backpropagation across the generator network, this technique is also computationally expensive.

Secure Water Treatment System

SWaT is a six-stage purification procedure used in the scaled-down water treatment testbed. It roughly resembles contemporary treatment facilities. It is used to research how to respond to cyberattacks and test out new security mechanism designs.

FIGURE .5: Visualization of SWaT testbed

A group of 28 sensors and 27 actuators manage the entire treatment procedure. Raw water is ingested and kept in a tank to start the process. In the second step, the pH and reduction potential of the water is adjusted by dosing chemicals like HCl, NaOCl, and NaCl in a static mixer. In the Ultra Filtration (UF) system's third step, contaminants are eliminated by passing through delicate membranes. The fourth step comes next, in which ultraviolet lights are used to dechlorinate the water. The water is then pushed through the Reverse Osmosis (RO) system in the fifth step to eliminate minor impurities. The water generated by RO is used in a backwashing procedure to clean the UF membrane. The RO system's clean water is stored and made ready for use in the final phase. A multilayer communications network, PLCs, HMIs, SCADA workstations, and a Historian make up the cyber component of SWaT.

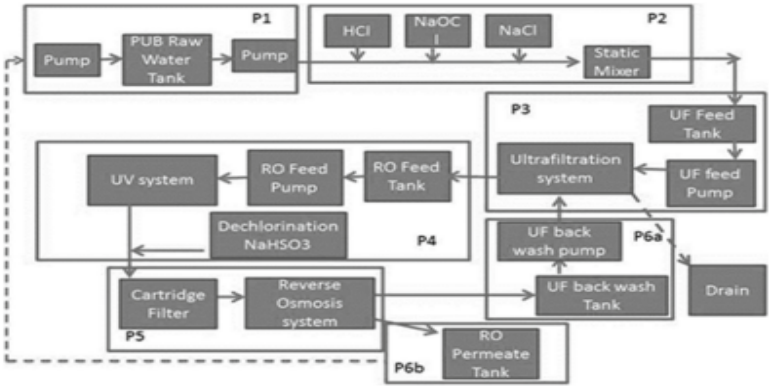

FIGURE .6: Architecture of the six-stage water treatment process. Credits: Siddhant Shrivastava, iTrust, SUTD

Water Distribution System

Water Distribution (WADI) is a realistic ICS testbed that simulates a water distribution network. It consists of a return tank which is used for water recycling, six consumer tanks, and two raised reservoir tanks for storage. It is managed by three PLCs and 103 sensors and actuators. The following phases are controlled by each PLC: P1 (Primary supply and analysis), P2 (Elevated reservoir with Domestic grid and leak detection), and P3 (Return process). The first step is to collect the raw water from the SWaT, the PUB inlet, or the return water from the WADI and store it in two tanks. Based on a predetermined demand pattern, P2 distributes water from two raised reservoir tanks and six consumer tanks. In the third step, reclaimed water is transferred back to P1.

FIGURE .7: Architecture of the Water Distribution System

Cyber Attacks

The SWaT and WADI system has been used in a number of tests to look at cyberattacks and the corresponding system responses. To learn more, please visit SWaT's and WADI's websites for an extensive the assaults' description. In the Secure Water Treatment System, the sensors and actuators were assaulted. Several related papers based on the SWaT dataset have been published as a testbed for cyber security research. Some of them concentrated on unique assaults. All of the aforementioned cyberattacks are treated as abnormal working circumstances in our study, and we train General Adversarial Networks to recognize these abnormalities for all six SWaT processes. For the WADI system, one attack objective is to interfere with the P1 water level sensor's readings. This can be shown by the following. The attacker changed the tank capacity sensor reading, which showed a "low status." The water supply from P1 to P2 was shut off at the same moment, but P2 kept supplying water to the consumer tanks due to the false low water level status in the raw water tank. Tank water levels in P2 therefore dropped. There would be an overflow in the tanks of P1 and no water flow in P2 as a result of changing the readings of the water level in sensor P1 to a low level.

SWaT Dataset

The SWaT data-collecting procedure took place over the course of 11 days, with the system running around the clock. The following traits apply to both the associated assaults and the SWaT dataset. Due to various conditions, different attacks may endure for varying amounts of time. Even some assaults don't start working right away. The times needed for system stabilization vary depending on the assault. Simpler attacks, including those that try to alter flow rates, take less time for the system to settle, but attacks that have a greater impact on the dynamics of the system would take longer. Attacks on one sensor may, generally after a short delay, have an impact on the performance of other sensors. Instead of treating each sensor or actuator in the ICS as a separate data source, we employ a multivariate approach to modeling.

WADI Dataset

The 1,209,610 records in the WADI dataset, each containing 123 characteristics broken down into 69 sensor readings and 54 actuator states, were gathered over the course of 16 days. For the first 14 days, normal operating conditions have been documented. As mentioned above in the SWAT dataset it is worthwhile to mention due to various conditions, different attacks may endure for varying amounts of time. Even some strikes did not instantly have an impact. The times needed for system stabilization vary depending on the assault. For example, one assault stops the flow of water to the consumer tanks, while another seeks to raise the concentration of chemicals in the water by turning off a sensor and giving the PLC false values for 10 minutes. Attacks on one sensor or actuator might have an impact on other sensors or actuators, or perhaps the entire system.

Experiments and Results

To compare the different models on the SWaT dataset we used the F1 score metric and the false positive rate for anomaly detection. The harmonic mean of recall and accuracy is used to get the F1 score. The formula to find the F1 score can be seen below.

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

The F1 Score's first component is precision. It is also applicable as a standalone machine-learning metric. The formula can be seen below.

$$Precision = \frac{\#\ of\ True\ Positives}{\#\ of\ True\ Positives + \#\ of\ False\ Positives}$$

The second factor in determining the F1 Score is recall, albeit recall may also be utilized as a standalone machine-learning statistic. The formula can be seen below.

$$Recall = \frac{\#\ of\ True\ Positives}{\#\ of\ True\ Positives + \#\ of\ False\ Negatives}$$

The false positive ratio is the likelihood that a specific test would incorrectly reject the null hypothesis. The ratio of the number of negative occurrences that were actually negative but were mistakenly classified as positive is used to compute the false positive rate. It can be derived with the following formula.

$$FPR = \frac{\mathbf{FP}}{\mathbf{FP} + \mathbf{TN}}$$

The SWaT dataset contains normal traffic and contains 36 kinds of attacks. There are 51 characteristics in the data set that is measured over 11 days. 400,000 of data samples were randomly selected and made into the training set and test set in the ratio of 3:1. Similarly, the WADI dataset also contains normal traffic and 15 kinds of attacks. There are 126 characteristics in the data set that is measured over 16 days. 125,000 data samples were randomly selected and made into the training set and test set in the ratio of 3:1. All conditions for the algorithms are the same wherever possible.

First, we compare 4 different machine learning and deep learning models on the SWaT data set

CNN - Convolutional Neural Network
RNN - Recurrent Neural Network
SVM - Support Vector Machine
DNN - Deep Neural Network

Model	F1	Precision	Recall
CNN	**0.813**	0.948	**0.712**
RNN	0.803	0.941	0.701
SVM	0.796	0.925	0.699
DNN	0.802	**0.982**	0.678

FIGURE .8: Performance on the SWaT dataset

The F1 score, precision, and recall for the algorithms SVM and DNN have been taken from the research paper "A Dataset to Support Research in the Design of Secure Water Treatment Systems" by Jonathan Goh, Sridhar Adepu, Khurum Nazir Junejo, and Aditya Mathur. As you can see from Table 1 CNN had the best F1 score with a score of 0.813 which is closely followed by RNN and DNN. The deep neural network had the best precision score of 0.982 and the CNN had the best recall score of 0.712. The table is shown in figure 8.

Multivariate Anomaly Detection – Generative Adversarial Network (MAD-GAN)
MAD-GAN is a multivariate time series of sensors and actuators that can be captured using an LSTM-RNN GAN under typical CPS operating circumstances. MAD-GAN models the time series of many sensors and actuators in the CPS simultaneously to account for potential latent interactions between them rather than addressing each sensor's and actuator's time series separately. It uses the residuals between the generator-reconstructed data and the actual samples, the GAN-trained discriminator, and both the generator and the discriminator of our GAN to detect potential anomalies in the complicated CPS. GAN-AD is utilized to differentiate between unusual attack scenarios and typical operating settings.

Evolutionary Generative Adversarial Networks (E-GAN)
Evolutionary Generative Adversarial Networks are a stable GAN framework for training and improved generative performance. E-GAN generates a population of generators to adapt to the environment, which serves as the discriminator, by using various adversarial training objectives as mutation operations. Additionally, it makes use of an assessment process to gauge the standard and variety of the samples that are created, ensuring that only the best generators are kept and put to use for additional training. By consistently preserving the finest progeny, E-GAN gets beyond the drawbacks of a single adversarial training objective and advances the development and effectiveness of GANs.

Encoder-Decoder Anomaly Detection (EncDec-AD)

Encoder-Decoder scheme for Anomaly Detection (EncDec-AD) is a Long Short Term Memory Network-based method that employs reconstruction error to find anomalies after learning to rebuild 'normal' time-series behavior. The decoder reconstructs the time series using the vector representation that the encoder learned for the input time series. The input time series itself serves as the target time series for the LSTM-based encoder-decoder, which has been trained to reconstruct instances of "regular" time series. The chance of an anomaly occurring at that location is then calculated using the reconstruction error at every subsequent time occurrence.

Transformer Based Generative Adversarial Network Anomaly Detection (TGAN-AD)

To elicit the performance, TGAN-AD collects contextual elements from time series data. The discriminator in TGAN-AD can help identify anomalous data. The transformer is used in an adversarial manner to understand anomalous patterns in time series data. The components of TGAN-AD are an anomaly detection component, a generator component, and a discriminator component. The generator component uses the Transformer to simulate normal patterns of time series data, and the discriminator component can capture intrinsic characteristics of real-time series data to learn the boundary between normal patterns and anomalous patterns.

Model	Precision	Recall	F1	FPR
MAD-GAN	**0.946**	0.759	**0.843**	0.31
E-GAN	0.885	0.669	0.762	0.23
EncDec-AD	0.867	0.583	0.697	0.22
TGAN-AD	0.862	**0.775**	0.816	0.36

FIGURE .9: Performance of Generative adversarial networks on the SWaT dataset

- MAD-GAN performed the best with the highest precision of 0.946. The other 3 models fairly had similar precisions ranging from 0.86-0.89 with the TGAN-AD having the least precision with 0.862
- Although having a slightly lower precision, TGAN-AD had the highest recall with 0.775. MAD-GAN had the second-highest recall score followed by E-GAN. EncDec-AD performed the worst with a recall score of just 0.583
- MAD-GAN performed the best on the SWaT dataset with an F1 score of 0.843 which TGAN-AD closely follows with an F1 score of 0.816. EncDec performed the worst with an F1 score of just 0.697
- EncDec-AD has the lowest false positive rate with 0.22. Although MAD-GAN has the highest F1 score, it has a fairly high false positive rate at 0.31. TGAN-AD has the highest false positive rate at 0.36

Model	Precision	Recall	F1	FPR
MAD-GAN	**0.946**	0.759	**0.843**	0.31
E-GAN	0.885	0.669	0.762	0.23
EncDec-AD	0.867	0.583	0.697	0.22
TGAN-AD	0.862	**0.775**	0.816	0.36

FIGURE .10: Performance of Generative adversarial networks on the WADI dataset

- The best performance came from TGAN-AD, which had a precision of 0.491. MAD-GAN performed similarly with a precision of 0.439. The other two models E-GAN and EncDec-AD had a much lower precision with EncDec-AD having the lowest
- TGAN-AD also had the highest recall by far with a recall of 0.449. E-GAN and EncDec had similar recalls with E-GAN performing slightly worse with the lowest recall of 0.171
- TGAN-AD performed the best on the WADI dataset with an F1 score of 0.469. MAD-GAN performed the second best with an F1 score of 0.384. E-GAN and EnCDec-AD have the lowest F1 scores with 0.223 and 0.240 respectively
- Although TGAN-AD has the highest precision, recall, and F1 score, it also has the highest false positive rate at 0.48. MAD-GAN has a false positive rate of 0.41. E-GAN has the lowest false positive rate at 0.21

Literature Review

There are quite a few datasets for the multivariate time series anomaly detection problem. There are also quite a few different algorithms for anomaly detection especially when it comes to general adversarial networks. We ran these models on the SWaT dataset and WADI dataset. I performed extensive background research in these concerned areas. All tests were run on an NVIDIA GeForce GTX 1060 3GB GDDR5 Graphics Card.

Conclusion and Future Work

In this work, we looked at a technique for finding group anomalies in time-series data. To deliver better goods and services to a global population, businesses and industries make decisions based on data. There are several options available when using analytical methods to extract useful information from huge amounts of data gathered from diverse sources. Time-series data may be used to detect and resolve unexpected events, which can assist avoid mishaps and monetary losses. Deep learning has recently been gaining attraction as it's a comprehensive field of study that can provide solutions to the problems of

anomaly detection. It has appeared that LSTM-based models have performed well on the multivariate time series data. As the complexity of data increases. Traditional models of machine learning are simply not enough to handle this work. The ever-growing complexity of deep learning models can help bridge the gap with ever-growing technology. There is still research to be done in the field of generative adversarial networks on multivariate anomaly detection on time series data. There is much room for improvement in these models in areas such as their efficiency, computational power, and accuracy, among others. The training of GANs may be challenging but the area is developing quickly, and society will immediately benefit from any innovations that speed up or stabilize training. A promising method for finding anomalies in complicated, high-dimensional data is GANs. Future research should be interested in applying GANs to additional data modalities, such as voice and sensor data.

Bibliography

[1] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” ACM Comp. Sur., vol. 41, p. 15:1:15:58, 2009.

[2] A. Zimek, E. Schubert, and H.-P. Kriegel, “A survey on unsupervised outlier detection in high-dimensional numerical data,” Stat. Anal. Data Min., vol. 5, pp. 363-387, 2012.

[3] M. A. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, “A review of novelty detection,” Signal Processing, vol. 99, pp. 215 – 249, 2014.

[4] Wang, Chu, Yan-Ming Zhang, and Cheng-Lin Liu. ”Anomaly detection via minimum likelihood generative adversarial networks.” 2018 24th International Conference on Pattern Recognition (ICPR). IEEE, 2018.

[5]Bulusu, Saikiran, et al. ”Anomalous example detection in deep learning: A survey.” IEEE Access 8 (2020): 132330-132347.

[6] Di Mattia, Federico, et al. ”A survey on gans for anomaly detection.” arXiv preprint arXiv:1906.11632 (2019).

[7] Schlegl, Thomas, et al. ”Unsupervised anomaly detection with generative adversarial networks to guide marker discovery.” International conference on information processing in medical imaging. Springer, Cham, 2017.

[8] Chalapathy, Raghavendra, and Sanjay Chawla. ”Deep learning for anomaly detection: A survey.” arXiv preprint arXiv:1901.03407 (2019).

[9] Li, Dan. (2018). Anomaly Detection with Generative Adversarial Networks for Multivariate Time Series.

[10] H. Zenati, M. Romain, C. -S. Foo, B. Lecouat and V. Chandrasekhar, "Adversarially Learned Anomaly Detection," 2018 IEEE International Conference on Data Mining (ICDM), 2018, pp. 727-736, doi: 10.1109/ICDM.2018.00088.

[11] Radford, Alec, Luke Metz, and Soumith Chintala. "Unsupervised representation learning with deep convolutional generative adversarial networks." arXiv preprint arXiv:1511.06434 (2015).

[12] B. Du, X. Sun, J. Ye, K. Cheng, J. Wang and L. Sun, "GAN-Based Anomaly Detection for Multivariate Time Series Using Polluted Training Set," in IEEE Transactions on Knowledge and Data Engineering, doi: 10.1109/TKDE.2021.3128667.

[13] B. J. Beula Rani and L. Sumathi M. E, "Survey on Applying GAN for Anomaly Detection," 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1-5, doi: 10.1109/ICCCI48352.2020.9104046.

[14] Li, Dan, et al. "MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks." International conference on artificial neural networks. Springer, Cham, 2019.

[15] X. Zhang, J. Wang and S. Zhu, "Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection," in IEEE Access, vol. 10, pp. 900-913, 2022, doi: 10.1109/ACCESS.2021.3128024.

[16] Vu, Ha Son, et al. "Anomaly detection with adversarial dual autoencoders." arXiv preprint arXiv:1902.06924 (2019).

[17] Moshe Kravchik and Asaf Shabtai. 2018. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy (CPS-SPC '18). Association for Computing Machinery, New York, NY, USA, 72–83. https://doi.org/10.1145/3264888.3264896

[18] Generative Adversarial Network (GAN) - https://www.geeksforgeeks.org/generative-adversarial-network-gan/

[19] Gray, Kathryn et al. "Coupled IGMM-GANs for deep multimodal anomaly detection in human mobility data." ArXiv abs/1809.02728 (2018): n. pag.

[20] Shalyga, Dmitry, Pavel Filonov, and Andrey Lavrentyev. "Anomaly detection for water treatment system based on neural network with automatic architecture optimization." arXiv preprint arXiv:1807.07282 (2018).

[21] Anomaly detection Using Generative Adversarial Networks(GAN) - https://medium.com/analytics-vidhya/anomaly-detection-using-generative-adversarial-networks-gan-ca433f2ac287

[22] Kopčan, Jaroslav Skvarek, Ondrej Klimo, Martin. (2021). Anomaly detection using Autoencoders and Deep Convolution Generative Adversarial Networks. Transportation Research Procedia. 55. 1296-1303. 10.1016/j.trpro.2021.07.113.

[23] Bulusu, Saikiran, et al. "Anomalous example detection in deep learning: A survey." IEEE Access 8 (2020): 132330-132347.

[24] C. Maru and I. Kobayashi, "Collective Anomaly Detection for Multivariate Data using Generative Adversarial Networks," 2020 International Conference on Computational Science and Computational Intelligence (CSCI), 2020, pp. 598-604, doi: 10.1109/CSCI51800.2020.00106.

[25] Balaji, M., Shrivastava, S., Adepu, S., Mathur, A. (2021). Super Detector: An Ensemble Approach for Anomaly Detection in Industrial Control Systems. In: Percia David, D., Mermoud, A., Maillart, T. (eds) Critical Information Infrastructures Security. CRITIS 2021. Lecture Notes in Computer Science(), vol 13139. Springer, Cham. https://doi.org/10.1007/978-3-030-93200-82

[26] Zhang, Chuxu et al. "A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series Data." ArXiv abs/1811.08055 (2018): n. pag.

[27] K. Choi, J. Yi, C. Park and S. Yoon, "Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines," in IEEE Access, vol. 9, pp. 120043-120065, 2021, doi: 10.1109/ACCESS.2021.3107975.

[28] Deng, Ailin, and Bryan Hooi. "Graph neural network-based anomaly detection in multivariate time series." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 35. No. 5. 2021.

[29] Xu, Liyan Xu, Kang Qin, Yinchuan Li, Yixuan Huang, Xingting Lin, Zhicheng Ye, Ning Ji, Xuechun. (2022). TGAN-AD: Transformer-Based GAN for Anomaly Detection of Time Series Data. Applied Sciences. 12. 8085. 10.3390/app12168085.

[30] Malhotra, Pankaj, et al. "LSTM-based encoder-decoder for multi-sensor anomaly detection." arXiv preprint arXiv:1607.00148 (2016).

[31] Xue, Feng, and Weizhong Yan. ”Multivariate Time Series Anomaly Detection with Few Positive Samples.” 2022 International Joint Conference on Neural Networks (IJCNN). IEEE, 2022.

[32] Wang, Chaoyue, et al. ”Evolutionary generative adversarial networks.” IEEE Transactions on Evolutionary Computation 23.6 (2019): 921-934.

[33] Abdelaty, Maged, Roberto Doriguzzi-Corin, and Domenico Siracusa. ”DAICS: A deep learning solution for anomaly detection in industrial control systems.” IEEE Transactions on Emerging Topics in Computing 10.2 (2021): 1117-1129.