

Detection of cyberattacks using bidirectional generative adversarial network

Rohith Vallabhaneni¹, Srinivas A. Vaddadi¹, Sanjaikanth E Vadakkethil Somanathan Pillai²,
Santosh Reddy Addula¹, Bhuvanesh Ananthan³

¹Department of Information Technology, University of the Cumberland, Williamsburg, United States

²School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, United States

³Department of Electrical and Electronics Engineering, PSN College of Engineering and Technology, Tirunelveli, India

Article Info

Article history:

Received Mar 16, 2024

Revised Apr 20, 2024

Accepted May 7, 2024

Keywords:

Communication technologies

Cyberattacks

Deep learning

Generative methods

Intrusion detection system

ABSTRACT

Due to the progress of communication technologies, diverse information is transmitted in distributed systems via a network model. Concurrently, with the evolution of communication technologies, the attacks have broadened, raising concerns about the security of networks. For dealing with different attacks, the analysis of intrusion detection system (IDS) has been carried out. Conventional IDS rely on signatures and are time-consuming for updation, often lacking coverage for all kinds of attacks. Deep learning (DL), specifically generative methods demonstrate potential in detecting intrusions through network data analysis. This work presents a bidirectional generative adversarial network (BiGAN) for the detection of cyberattacks using the IoT23 database. This BiGAN model efficiently detected different attacks and the accuracy and F-score values achieved were 98.8% and 98.2% respectively.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Rohith Vallabhaneni

Department of Information Technology, University of the Cumberland

College Station Drive, Williamsburg, KY 40769, United States

Email: rohit.vallabhaneni.2222@gmail.com

1. INTRODUCTION

The term cybersecurity encompasses a broad scope, typically involving the analysis and development of security protocols designed to safeguard digital systems connected through the internet. The past few decades have seen a significant transformation in the digital realm, as technological progress has become ubiquitous in our daily lives [1]. These advancements, while providing unparalleled accessibility and connectivity have also unveiled new challenges and vulnerabilities for society to contend with. The occurrence and complexity of cybercrimes have increased significantly, defining the digital era through noteworthy incidents that have deeply affected industries and the world. Due to the advancement of 5G networks, characterized by diversified access environments and the establishment of dispersed networks, facilitates the communication of diverse and heterogeneous data through networks [2].

Typically, these data emerge from various fields like sensors, and the internet of things (IoT) and the potential of networks is enlarged. As access points diversify, the attack surface expands, rendering network systems more susceptible to potential attacks. Additionally, cyberattack approaches are complicated and advanced, which results in more attacks [3]. Consequently, the significance of cybersecurity is underscored, leading to active research and studies aimed at preventing network threats. In response to potential threats, extensive analysis is pursued in the domain of intrusion detection system (IDS). Anomaly detection models based on artificial intelligence (AI) have garnered recent attention as a promising avenue within the realm of

IDS technologies. Numerous models are developed to enhance IDS performance. But, a persistent challenge remains in the form of data balancing issue, wherein AI methods struggle to effectively learn malicious behavior, leading to suboptimal detection of network threats [4].

A major issue in the cybersecurity detection revolves around identifying network threats, and numerous findings have been documented concerning IDS. Notably, recent research has prominently centered on the integration of the AI approach into IDS [5]. Machine learning (ML) techniques are extensively employed in constructing IDS to swiftly and automatically detect and classify cyberattacks. Nonetheless, numerous limitations emerge due to the evolving nature of malicious attacks and their occurrence in vast volumes, necessitating scalable solutions. The outcomes indicate that AI based IDS have demonstrated noteworthy achievement [6]. The conventional ML approaches like support vector machine (SVM) and random forest (RF) were exploited to identify intrusions. These ML approaches are modified as deep learning (DL) like convolutional neural network autoencoder (CNN) and long short term memory (LSTM) [7]. Typically, the majority of network flow data constitutes normal traffic, with instances of malicious behavior leading to service failure being infrequent. Furthermore, among the malicious activities, a significant portion comprises well-known attacks, while specific types of attacks are exceedingly rare. The challenge arises from the imbalance in data distribution, causing AI models implemented in IDS to inadequately grasp the distinctive features of particular network threats. Consequently, this imbalance may expose network systems to vulnerabilities, resulting in inaccurate performance [8]. The foremost contributions are:

- To present the latest dataset exclusively associated with behaviors related to IoT-based attacks, omitting the behaviors characteristic of conventional models.
- The study emphasizes an exhaustive analysis of various attacks by training the proposed BiGAN model as comprehensively as possible.

The remainder of the paper is structured as follows: Section 2 encompasses a review of the most pertinent literature in the realm of AI. Section 3 outlines the proposed methodology employed in this work. The experimental segment in section 4 and lastly, section 5 encapsulates the conclusion of the entire study.

2. RELATED WORKS

Abdalgawad *et al.* [9] presented adversarial autoencoder (AAE) and BiGAN for detecting intrusion. The pre-processing and the feature selection processes were carried out. The experimentation was carried out on the IoT-23 dataset and achieved a better F-score value of 0.85.

Khaw *et al.* [10], the researchers developed a DL based deep neural network (DNN) for IDS. Experimentation was carried out on the network and host IDS to identify the behaviour of network was malicious or normal. Performance was carried out by varying the DNN layers from 1 to 5 achieving a better F-score of 0.79 on the NSL-KDD dataset.

Azumah *et al.* [11] presented that IDS within a smart home's IoT device network relies on a DL approach specialized in detecting and categorizing attacks to ensure the security of IoT devices. This approach centers on LSTM for its substantial performance in addressing temporal dependencies and effectively handling intricate attack scenarios. Accuracy, precision and recall values achieved were 0.97, 0.8 and 0.75.

Liu *et al.* [12], the authors introduced the IDS model using hierarchical attention based gated recurrent unit (GRU). Attention probability mapping was utilized for reflecting the essential features. The FAR and the accuracy values achieved were 1.2% and 98.7% respectively. Alabugin and Sokolov [13] the authors presented GAN for detecting anomalies in industrial control system (ICS). The suggestion was to employ the BiGAN model for anomaly detection. This existing methodology was tested by the secure water treatment (SWaT) dataset.

Ullah and Mahmoud [14], the researchers suggested a conditional GAN model for detecting anomalies in IoT networks. An one-class GAN (oc-GAN) was employed to understand the minority data class, ensuring dataset balance. Subsequently, the binary class GAN (bc-GAN) model was utilized to produce augmented data for the balanced binary dataset. At last, the accuracy and precision values achieved were 95.4% and 95.5% on the NSL-KDD dataset.

Cai *et al.* [15] a very thorough and comprehensive model of the security and privacy aspects is modeled where GANs can be used. This paper fiercely presents the opposing views of GAN research. We look at situations in which the generator defends itself against the attacking discriminator (such as [16]-[19]), and situations in which the generator is an attacker against the defending classifier (such as [20]-[24]).

3. PROPOSED METHOD

This work presents a BiGAN model for detecting cyberattacks on the IoT23 database. Figure 1 depicts the flowchart of the proposed cyberattack detection model. In this analysis, to tackle the inherent

issue at hand, we introduce a pioneering generative DL based IDS designed to mitigate the challenges associated with data imbalance, thereby enhancing the efficacy of existing models. In response to the previously mentioned challenge, we have employed a BiGAN for generating traffic data for the network.

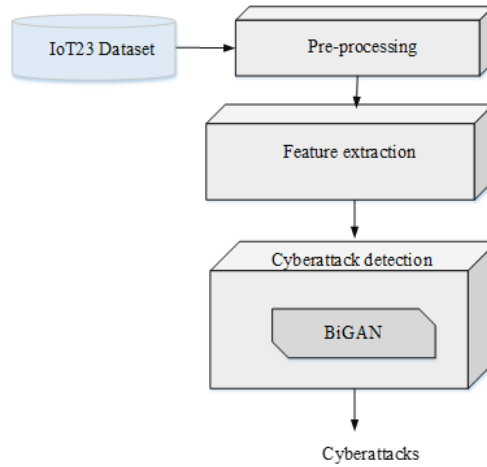


Figure 1. Flowchart of the proposed cyberattack detection model

3.1. Database

This study employed the IoT23 database, obtained for training and testing purposes, and sourced from [25]. This database originates from IoT network traffic, illustrating communicating patterns in three benign IoT devices and twenty samples involving malware executed on IoT devices. Comprising 21 instances, the dataset includes a final feature serving as the label. It is designated as a multilabel dataset, with every label potentially associated with various kinds of attacks.

3.2. Pre-processing

The initial phase of the proposed attack detection model is pre-processing. Here, eliminate redundant attributes from data instances and the categorical features are transformed to one hot vector model. Then, the normalization process is performed to standardize the data and it is given as:

$$Y_{norm} = \frac{Y - \min(z)}{\max(z) - \min(z)} \tag{1}$$

where $\min(z)$ and $\max(z)$ are the minimum and maximum values having an attribute z .

3.3. Cyberattack detection using the BiGAN

For building a cyberattack detection model, the BiGAN is trained and tested. The BiGAN estimates generative model G by the adversarial technique training a G for capturing the distribution of data and the discriminator D that defines the rate that a sample of data arrives from the train set or is produced using G . The standard GAN model is used for training G and D simultaneously so that D enhances the rate of providing accurate label for the sample produced from G and train set from data y .

$$\min_G \max_D U(D, G) = E_{y \sim Q_{data}(y)} [\log D(y)] + E_{a \sim Q(a)} [\log(1 - D(y))] \tag{2}$$

Where $y \sim Q_{data}(y)$ is the distribution of data, $E_{a \sim Q(a)}$ is the noisy parameter and $U(D, G)$ is function term. Figure 2 defines the BiGAN model which has an encoder E and is used for mapping y for the latent indication x . The training model E is used to represent features with respect to semantics. In contrast to the GAN, the D in the BiGAN discriminates between pairs $(y, E(y))$ and $(x, G(x))$. The training model of the BiGAN is given as (3).

$$\min_{G,E} \max_D U(D, G, E) = E_{y \sim Q_{data}(y)} [\log D(y, E(y))] + E_{a \sim Q(a)} [\log(1 - D(G(x), x))] \tag{3}$$

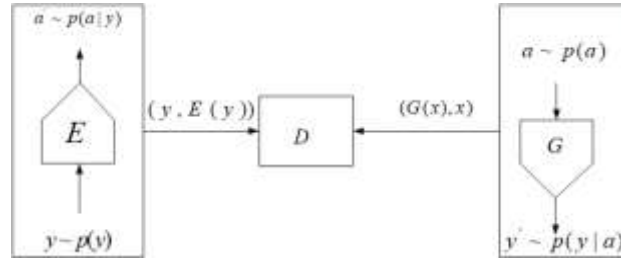


Figure 2. Structure of BiGAN model

The training procedure for detection of cyberattack model of BiGAN is given as: the E and G should effectively invert one another to deceive the D . In the BiGAN model, the E and G exhibit behavior same like to the encoding and decoding of an autoencoder (AE). This AE is designed to learn a representation for a given set of input data and subsequently reconstruct the samples of data as near as feasible to the original input values. To enhance training of BiGAN, we incorporate the reconstruction variation among the input g and its reconstructed counterpart $(GE(y))$, calculated by the L_2 norm through the E and G . This technique provides additional assistance to the training process, augmenting the model's ability for reconstructing input.

$$L_r = \frac{1}{n_y} \|y - (GE(y))\|_2 \quad (4)$$

Where n_y is the input values. In their methodology, these cues are seamlessly integrated into the BiGAN loss function. This study, on the other hand, integrates hints at regular intervals to optimize training efficiency further. Furthermore, within the D , the DL model immediately preceding the last layer is designated as a vector of feature f_e . Leveraging this D -derived f_e , an extra hint loss is delineated as part of the approach, ensuring a comprehensive and nuanced training process.

$$L_{f_e} = \frac{1}{n_{f_e}} \|f_e(y, E(y)) - f_e(GE(y), E(y))\|_2 \quad (5)$$

Where n_{f_e} is the neuron's features. Integrating the L_r and L_{f_e} , the loss function of hint L_h is given as:

$$L_h = \frac{l}{n_y} \|y - (GE(y))\|_2 + \frac{1}{n_{f_e}} \|f_e(y, E(y)) - f_e(GE(y), E(y))\|_2 \quad (6)$$

where l is the hyperparameter. Here, total number of epochs considered are 160, the latent dimension considered is 32, there are 3 layers in the D , activation function considered in D and E are ReLU. In both GAN and BiGAN models, the G 's connection to the loss function is established indirectly through the D . The desired loss, aimed at minimization, is derived from the G , the E , and the D , all of which are fed by the G and E . The G faces penalties for generating samples classified as fake by the D . The impact of the G 's variable is based on the D 's variables, which are influenced by the G . Consequently, the back-propagation initiates from the D 's output and traverses through the D to reach the G . Notably, during this phase of the training, the D remains unaltered. The reciprocal dependence between G and D poses a challenging task for training and, particularly, exacerbates the difficulty for the G component. The loss function is given as (7).

$$MSE = \frac{1}{m} \sum_{j=1}^m (y_j - G(a_j))^2 \quad (7)$$

4. RESULTS ANALYSIS

A 10-fold sampling strategy was utilized for assessment, creating training and testing sets at each split. After generating the training set, normalization and balancing, as described earlier, were implemented. Following these steps, diverse classifiers and GANs underwent training on the prepared training data. This procedure involves partitioning the database into two distinct sets: a training subset and a testing subset. Despite the direct utilization of these subsets as inputs for the DL models, this step is deemed part of the preprocessing activities. In this study, 20% of the dataset is earmarked for the testing phase, while the remaining 80% is allocated for the training phase. The extraction of samples from the dataset for training and testing purposes has been executed in a random fashion. Table 1 indicates the performance metrics which include Accuracy, precision, sensitivity, specificity, and F-score respectively.

Table 1. Performance metrics

Metrics	Expressions
Accuracy	$\frac{S_{po} + S_{ne}}{S_{po} + S_{ne} + R_{po} + R_{ne}}$
Precision	$\frac{S_{po}}{S_{po} + R_{po}}$
Sensitivity	$\frac{S_{po}}{S_{po} + R_{ne}}$
F-score	$\frac{S_{po}}{S_{po} + R_{po} + R_{ne}}$
Specificity	$\frac{S_{po} + S_{ne}}{S_{po} + S_{ne} + R_{po} + R_{ne}}$

where S_{po} and S_{ne} , R_{po} and R_{ne} represents the true and false positives, false and true negatives.

4.1. Comparative analysis

In this section, initially the performance of the proposed BiGAN is given. Then, the comparative analysis is presented for various approaches. Table 2 depicts the performance of the proposed cyberattack detection model. Here, the performance is evaluated for the classes like Benign, Attack, C&C, DDoS, Okiru, File_download, and C&C-HeartBeat. The experimental assessment in this study relies on the k-fold method, wherein the database is partitioned into 10 subsets. In each iteration, 1-subset is utilized for testing, while the remaining 9-subsets are employed for training. Figure 3 shows the performance analysis by varying the fold values. Figure 3(a) presents the Accuracy, Precision, and F-score by varying the fold values of the proposed cyberattack detection model. Similarly, Figure 3(b) presents the sensitivity and specificity by varying the fold values. Across all fold values, it is noted that the suggested cyberattack detection model consistently achieved superior results.

Table 2. Performance of the proposed cyberattack detection model

Classes	Accuracy	Precision	Sensitivity	Specificity	F-score
Benign	98.9	97.9	97.5	94.1	99.2
Attack	98.9	97.9	97.2	99.3	99.1
C&C	99.3	98.7	99.1	99.1	98.8
DDoS	98.2	98.9	99.3	98.9	98.2
Okiru	96.9	96.1	98.3	99.0	98.7
File_download	99.1	99.2	98.7	98.2	99.1
C&C-HeartBeat	99.9	92.3	98.4	99.1	98.4

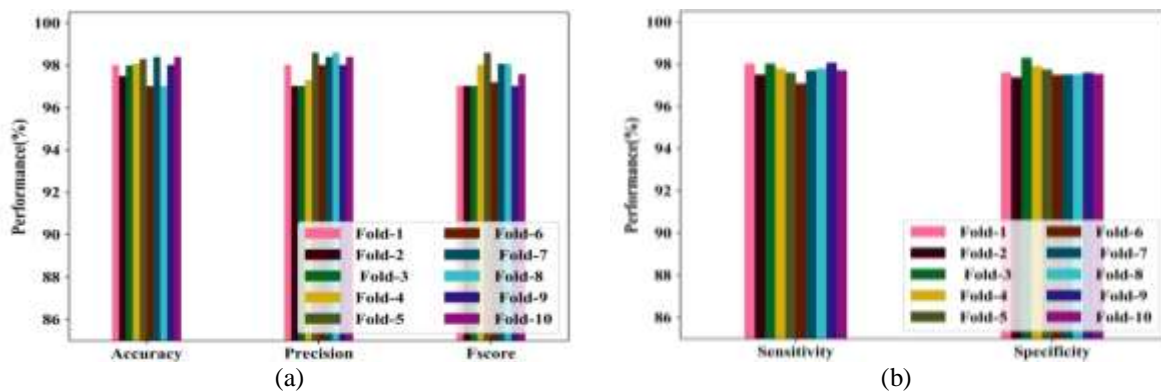


Figure 3. Performance by varying the fold values (a) accuracy, precision and F-score and (b) sensitivity and specificity

Figure 4 delineates the confusion matrix of the proposed cyberattack detection model. In this, class 1 is the Benign, class 2 is the Attack, class 3 is the C&C, class 4 is the DDoS, class 5 is the Okiru, class 6 is the File_download and class 6 is the C&C-HeartBeat. The proposed cyberattack detection model identified 500 samples as 1, 431 samples as 2, 300 samples as 3, 300 samples as 4, 110 samples as 5, 5 samples as 6 and 1 sample as 7. The accuracy-loss curves for the proposed method is illustrated in Figure 5. Figure 5(a) presents the accuracy curves, and Figure 5(b) presents the loss curves of the proposed cyberattack detection model. In the

graphical representation, different epoch's values are plotted on the X-axis, while the values of accuracies and losses are plotted on the Y-axis. A comprehensive training of 160 epochs is conducted. The green and blue curves illustrate the training and validation curves, respectively. Notably, the training loss achieved stability after approximately 100 epochs, while the validation loss stabilized around the 80th epoch. Both training and validation accuracies exhibited a gradual increase, ultimately converging towards 0.98.

Table 3 depicts the comparative analysis of the different ML and DL models. The models like RF, SVM, LSTM, BILSTM, AE, and GAN are compared with the proposed cyberattack detection model. It is observed that the proposed cyberattack detection model is superior over the conventional models. The ML techniques, including GANs, offer the potential to detect novel and sophisticated cyber threats that traditional rule-based methods might miss. GANs, in particular, can generate synthetic data that can be used to augment training datasets, which is beneficial in scenarios where real attack data is limited or difficult to obtain. The adversarial nature of GANs makes them suitable for modeling complex, evolving cyber threats. The benefits of using BiGANs for cyberattack detection include improved accuracy, reduced false positives, adaptability to dynamic environments, data augmentation, real-time detection, enhanced security posture, privacy preservation, and complementarity with existing solutions. These advantages make BiGANs a valuable tool in the arsenal of cybersecurity defenses, particularly in detecting and mitigating advanced threats.

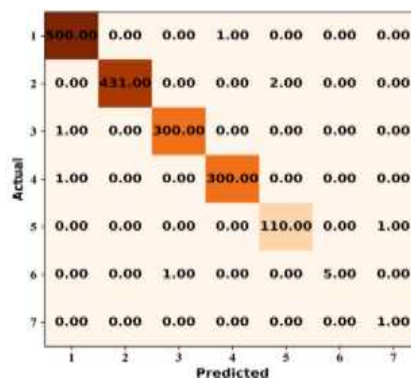


Figure 4. Confusion matrix of the proposed cyberattack detection model

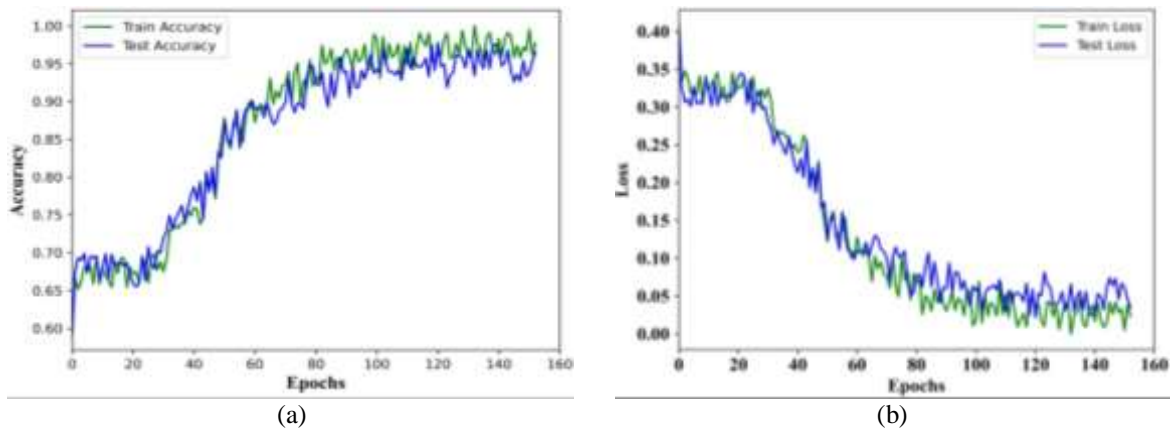


Figure 5. Accuracy-loss curve (a) accuracy curves and (b) loss curves of the proposed cyberattack detection model

Table 3. Comparative analysis

Methods	Accuracy	Precision	Sensitivity	Specificity	F-score
RF	78.4	87.2	91.2	91.4	89.7
SVM	81.2	88.7	91.7	93.5	90.4
LSTM	83.4	89.3	93.2	94.2	92.3
BILSTM	87.2	93.1	94.3	95.3	94.5
AE	88.4	94.1	94.8	96.4	95.4
GAN	93.1	97.2	95.5	96.9	96.3
Proposed	98.8	98.2	98.5	98.2	98.2

5. CONCLUSION

This research introduces an innovative generative DL based IDS model for effectively addressing cyberattacks and enhancing the performance of classification. This work presented the BiGAN model for classifying various types of cyberattacks. The experimentation was carried out on the IoT23 database and it undergoes stages like pre-processing and cyberattack detection using the BiGAN. Different performance measures were carried out by varying k-folds and attained better outcomes. This experimental analysis illustrates that the suggested model can notably enhance the network threat detection rate. In the future, we aim to adapt our framework to practical implications, with a specific emphasis on its application in federated learning models for enhancing the network threat detection. Furthermore, our future endeavors will include an exploration of adversarial attacks capable of circumventing generative DL based IDS by exploiting vulnerable activities in DL models. We plan to conduct research on IDS that can effectively counteract these attacks within real time models.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.





REFERENCES

- [1] S. Oh, and T. Shon, "Cybersecurity issues in generative AI," *In 2023 International Conference on Platform Technology and Service (PlatCon)*, IEEE, pp. 97-100, 2023, doi: 10.1109/platcon60102.2023.10255179.
- [2] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, 2024, doi: 10.1016/j.iotcps.2023.12.003.
- [3] C. Yinka-Banjo, and O. A. Ugot, "A review of generative adversarial networks and its application in cybersecurity," *Artificial Intelligence Review*, vol. 53, pp. 1721-1736, 2020, doi: 10.1007/s10462-019-09717-4.
- [4] M. Chalé, and N. D. Bastian, "Generating realistic cyber data for training and evaluating machine learning classifiers for network intrusion detection systems," *Expert Systems with Applications*, vol. 207, pp. 117936, 2022, doi: 10.1016/j.eswa.2022.117936.
- [5] P. Jisna, T. Jarin, and P. N. Praveen, "Advanced intrusion detection using deep learning-LSTM network on cloud environment," *In 2021 Fourth International Conference on Microelectronics, Signals and Systems (ICMSS)*, IEEE, pp. 1-6, 2021, doi: 10.1109/icmss53060.2021.9673607.
- [6] I. A. Khan, D. Pi, P. Yue, B. Li, Z. U. Khan, Y. Hussain, and A. Nawaz, "Efficient behaviour specification and bidirectional gated recurrent units-based intrusion detection method for industrial control systems," *Electronics Letters*, vol. 56, no. 1, pp. 27-30, 2020, doi: 10.1049/el.2019.3008.
- [7] A. AlErroud, Ahmed, and G. Karabatis, "Sdn-gan: generative adversarial deep NNS for synthesizing cyber-attacks on software defined networks," *In on the Move to Meaningful Internet Systems: OTM 2019 Workshops: Confederated International Workshops: EI2N, FBM, ICSP, Meta4eS and SIAna 2019*, Rhodes, Greece, Springer International Publishing, October 21–25, 2019, pp. 211-220, 2020, doi: 10.1007/978-3-030-40907-4_23.
- [8] F. Li, H. Shen, J. Mai, T. Wang, Y. Dai, and X. Miao, "Pre-trained language model-enhanced conditional generative adversarial networks for intrusion detection," *Peer-to-Peer Networking and Applications*, pp. 1-19, 2023, doi: 10.1007/s12083-023-01595-6.
- [9] N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan, and F. Aloul, "Generative deep learning to detect cyberattacks for the IoT-23 dataset," *IEEE Access*, vol. 10, pp. 6430-6441, 2021, doi: 10.1109/ACCESS.2021.3140015.
- [10] Y. M. Khaw, A. A. Jahromi, M. F. Arani, S. Sanner, D. Kundur, and M. Kassouf, "A deep learning-based cyberattack detection system for transmission protective relays," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2554-2565, 2020, doi: 10.1109/TSG.2020.3040361.
- [11] S. W. Azumah, N. Elsayed, V. Adewopo, Z. S. Zaghoul, and C. Li, "A deep lstm based approach for intrusion detection iot devices network in smart home," *In 2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, IEEE, pp. 836-841, 2021, doi: 10.1109/wf-iot51360.2021.9596033.
- [12] C. Liu, Y. Liu, Y. Yan, and J. Wang, "An intrusion detection model with hierarchical attention mechanism," *IEEE Access*, vol. 8, pp. 67542-67554, 2020, doi: 10.1109/ACCESS.2020.2983568.
- [13] S. K. Alabugin, and A. N. Sokolov, "Applying of generative adversarial networks for anomaly detection in industrial control systems," *In 2020 Global Smart Industry Conference (GloSIC)*, IEEE, pp. 199-203, 2020, doi: 10.1109/glosic50886.2020.9267878.
- [14] I. Ullah, and Q. H. Mahmoud, "A framework for anomaly detection in IoT networks using conditional generative adversarial networks," *IEEE Access*, vol. 9, pp. 165907-165931, 2021, doi: 10.1109/ACCESS.2021.3132127.
- [15] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, "Generative adversarial networks: a survey toward private and secure applications," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–38, 2021, doi: 10.1145/3459992.
- [16] S. Baluja, and I. Fischer, "Adversarial transformation networks: Learning to generate adversarial examples," *arXiv preprint arXiv:1703.09387*, 2017, doi: 10.1609/aaai.v32i1.11672.
- [17] Y. Gao, and Y. Pan, "Improved detection of adversarial images using deep neural networks," *arXiv preprint arXiv:2007.05573*, 2020, doi: 10.1063/pt.5.028530.
- [18] B. Hitaj, G. Ateniese, and F. Perez-Cruz, "Deep models under the gan: information leakage from collaborative deep learning," *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 603–618, 2017, doi: 10.1145/3133956.3134012.
- [19] Z. Zhao, D. Dua, and S. Singh, "Generating natural adversarial examples," *arXiv preprint arXiv:1710.11342*, 2017, doi: 10.1063/pt.5.028530.
- [20] X. Chen, P. Kairouz, and R. Rajagopal, "Understanding compressive adversarial privacy," *in 2018 IEEE Conference on Decision and Control (CDC)*, pp. 6824–6831, IEEE, 2018, doi: 10.1109/cdc.2018.8619455.
- [21] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Contextaware generative adversarial privacy," *Entropy*, vol. 19, no. 12, pp. 656, 2017, doi: 10.3390/e19120656.





- [22] S. Liu, A. Shrivastava, J. Du, and L. Zhong, "Better accuracy with quantified privacy: representations learned via reconstructive adversarial network," *arXiv preprint arXiv:1901.08730*, 2019, doi: 10.1002/leap.1229.
- [23] A. Tripathy, Y. Wang, and P. Ishwar, "Privacy-preserving adversarial networks," in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 495–505, 2019, doi: 10.1109/allerton.2019.8919758.
- [24] K. Alrawashdeh, and S. Goldsmith, "Defending deep learning based anomaly detection systems against white-box adversarial examples and backdoor attacks," *International Symposium on Technology and Society, Proceedings*, vol. 2020-November, pp. 294–301, 2020, doi: 10.1109/istas50296.2020.9462227.
- [25] IoT23-dataset. <https://www.kaggle.com/datasets/astralfate/iot23-dataset>, doi: 10.7717/peerj-cs.456/fig-9.

BIOGRAPHIES OF AUTHORS







Dr. Rohith Vallabhaneni     received his Ph.D. degree in Information Technology from the University of the Cumberland in the United States. As a Senior IEEE member, he has contributed significantly to various research journals, both as an author and co-author. His professional journey is marked by a strong work ethic and a profound ability to lead teams in addressing organizational challenges. His exemplary team leadership skills and dedication to his work underscore his contributions to the field of Information Technology. He can be contacted at email: rohit.vallabhaneni.2222@gmail.com.







Srinivas A. Vaddadi     is a dynamic and forward-thinking professional in the field of Cloud and DevSecOps. With a solid educational foundation in computer science, Srinivas embarked on a journey of continuous learning and professional growth. Their relentless pursuit of knowledge and commitment to staying at the forefront of industry advancements has earned them recognition as a thought leader in the Cloud and DevSecOps space. He can be contacted at email: Vsad93@gmail.com.







Sanjaikanth E Vadakkethil Somanathan Pillai     (Senior Member, IEEE) holds an MS in Software Engineering from The University of Texas at Austin, Texas, USA, and a BE from the University of Calicut, Kerala, India. Currently pursuing a PhD in Computer Science at the University of North Dakota, Grand Forks, North Dakota, USA, his research spans diverse areas such as mobile networks, network security, privacy, location-based services, and misinformation detection. He is a proud member of Sigma Xi, the scientific research honor society, underlining his commitment to advancing scientific knowledge and research excellence. He can be contacted at email: s.evadakkethil@und.edu.



Santosh Reddy Addula     holds a master's degree in Information Technology from the University of the Cumberland in Kentucky, United States of America. He has over five years of experience working in the IT industry, and he has showcased expertise across various domains in IT. He has 3+ patents, has contributed as an author and co-author of research articles, and has a role as a reviewer for esteemed journals such as IEEE, Springer, and Elsevier. He can be contacted at email: santoshaddulait@gmail.com.



Dr. Bhuvanesh Ananthan     received the B.E. degree in Electrical and Electronics Engineering from Anna University in 2012, M.Tech. in Power System Engineering from Kalasalingam University in 2014 and Ph.D. degree from Faculty of Electrical Engineering of Anna University in 2019. He has published more than 65 papers in reputed international journals, 25 papers in international conferences and 10 books. He is a life time member of International Society for Research and Development, International Association of Engineers. He can be contacted at email: bhuvanesh.ananthan@gmail.com.