Detection of Cyber attack in IOT- enabled cyber physical systems

[1]S.VidyaLaxmi, [2]A.Anjali, [3] G.Manasa, [4]K.Sangeetha, [5]Dr. R. Jegedeesan, [6]Dr. M Sujatha, [7]K.Sai Venna

IV Year CSE Students[1,2,3,4]Associate Professor[5,6,7]

Jyothishmathi Institute of Technology And Science, Karimnagar, 505 481, Telangana.

ABSTARCT

Securing Internet of Things (IoT)-enabled cyber- physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT/ OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a deci- sion tree combined with a novel ensemble deep representation- learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

Index Terms—Cyber-attacks, Deep representation learning, Cyber threat detection, Cyber threat attribution, Industrial Control System, ICS, Cyber-physical systems, Industrial Internet of Things (IIoT)

1.INTRODUCTION

Internet of Things (IoT) devices are increasingly integrated in cyber-physical systems (CPS), including in critical infrastructure sectors such as dams and utility plants. In these settings, IoT devices (also referred to as Industrial IoT or IIoT) are often part of an Industrial Control System (ICS), tasked with the reliable operation of the infrastructure. ICS can be broadly defined to include supervisory control and data acquisition (SCADA) systems,

distributed control systems (DCS), and systems that comprise programmable logic controllers (PLC) and Modbus protocols.

The connection between ICS or IIoT-based systems with public networks, however, increases their attack surfaces and risks of being targeted by cyber criminals. One high-profile example is the Stuxnet campaign, which reportedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing severe damage to the equipment. Another example is that of the incident targeting a pump that resulted in the failure of an Illinois water plant in 2011. Black Energy was another campaign that targeted Ukraine power grids in 2015, resulting in power outage that affected approximately 230,000 people. In April 2018, there were also reports of successful cyber-attacks affecting three U.S. gas pipeline firms, and resulted in the shutdown of electronic customer communication systems for several days. Although security solutions developed for information technology (IT) and operational technology (OT) systems are relatively mature, they may not be directly applicable to ICSs. For example, this could be the case due to the tight integration between the controlled physical environment and the cyber systems.

Therefore, system-level security methods are necessary to analyse physical behaviour and maintain system operation availability. ICS security goals are prioritized in the order of availability, integrity, and confidentiality, unlike most IT/OT systems (generally prioritized in the order of confidentiality, integrity, and availability). Due to close coupling between variables of the feedback control loop and physical processes, (successful) cyber-attacks on ICS can result in severe and potentially fatal consequences for the society and our environment. This reinforces the importance of designing extremely robust safety and security measurements to detect and prevent intrusions targeting ICS.

2. LITERATURE REVIEW

1. Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data

Authors:F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble

Journal:IEEE,(2019)

The growing number of attacks against cyber-physical systems in recent years elevates the concern for cybersecurity of industrial control systems (ICSs). The current efforts of ICS cybersecurity are mainly based on firewalls, data diodes, and other methods of intrusion

prevention, which may not be sufficient for growing cyber threats from motivated attackers. To enhance the cybersecurity of ICS, a cyber-attack detection system built on the concept of defense-in-depth is developed utilizing network traffic data, host system data, and measured process parameters. This attack detection system provides multiple-layer defense in order to gain the defenders precious time before unrecoverable consequences occur in the physical system. The data used for demonstrating the proposed detection system are from a real-time ICS testbed. Five attacks, including man in the middle (MITM), denial of service (DoS), data exfiltration.

2. **Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber-Physical System.**

Authors: R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei

Journal:IEEE,(2019)

In an industrial cyber-physical system (ICPS), the controller plays a critical role in guaranteeing reliability and stability. Therefore, redundant controller architecture is a well-adopted approach by distributed control systems (DCS), supervisory control and data acquisition (SCADA), and other typical ICPSs. They monitor and control the critical industrial process, such as power generation, chemical industry, water treatment plant, etc. Redundant controller architecture has been designed and largely implemented in response to unpredictable mechanical failures. However, this structure initially proposed for guaranteeing reliability and safety may expand the cyber-attack surface, posing the risk that an attacker may take advantage of this architecture for stealthy attacks. In this article, we analyze the vulnerability arising from the redundant controller architecture and propose a combined attack methodology against these.

3.METHODOLOGY

Modules:

1. Data Owner

Data Owners are either individuals or teams who make decisions such as who has the right to accessand edit data and how its used. The data owner claims the possession and copyrights to such data toensure their control and ability to take legal action. A Data Owner is accountable for who hasaccess to information assets within their functional areas. A Data

Owner may decide to reviewand authorize each access request individually or may define a set of rules that determine whois eligible for access based on business function.

2. End User

The user is divided into two categories. One is the initial user who uploads files that did not exist in the cloud previously. The other one is the subsequent users who upload files that the IOT Sub Server kept. The initial user generates the authenticators for each encrypted file, then uploads the encrypted file, its corresponding authenticators and the file tag to the IOT Server. The subsequent user does not need to generate the data authenticators and upload the above messages to the IOT Server. Later, both the data owner and the End user can recover their data after downloading the data from the cloud. In addition, users are able to verify the integrity of the cloud data by executing the cloud storage auditing protocol with the cloud.

3. IOT Server

The IOT Server enormous storage space, and supplies storage services and downloading services for users. In order to improve storage efficiency, the IOT Server performs deduplication for duplicated files. In other words, the IOT Server keeps only a single copy of any duplicated le and its corresponding authenticators, and provides user with a link to the corresponding file.

4. IOT Sub Server

The IOT Server enormous storage space, and supplies storage services and downloading services for users. In order to improve storage efficiency, the IOT Server performs deduplication for duplicated files. In other words, the IOT Server keeps only a single copy of any duplicated le and its corresponding authenticators, and provides user with a link to the corresponding file.

5.IMPLEMENTATION

The varied topic in existence in the fields of computers, Client Server is one, which has generated more heat than light, and also more hype than reality. This technology has acquired a certain critical mass attention with its dedication conferences and magazines. Major computer vendors such as IBM and DEC, have declared that Client Servers is their main future market. A survey of DBMS magazine reveled that 76% of its readers were

actively looking at the client server solution. The growth in the client server development tools from $200 million in 1992 to more than $1.2 billion in 1996.

Client server implementations are complex but the underlying concept is simple and powerful. A client is an application running with local resources but able to request the database and relate the services from separate remote server. The software mediating this client server interaction is often referred to as MIDDLEWARE.

The typical client either a PC or a Work Station connected through a network to a more powerful PC, Workstation, Midrange or Main Frames server usually capable of handling request from more than one client. However, with some configuration server may also act as client. A server may need to access other server in order to process the original client request.

The key client server idea is that client as user is essentially insulated from the physical location and formats of the data needs for their application. With the proper middleware, a client input from or report can transparently access and manipulate both local database on the client machine and remote databases on one or more servers. An added bonus is the client server opens the door to multi-vendor database access indulging heterogeneous table joins.

4.DATASET

we evaluated the proposed frame- work using two real-world ICS datasets. The first dataset was collected at the Mississippi State University [23] froma gas pipeline system consisting of sensors and actuators, a communication network, and supervisory control. This dataset consistsofnormalsamplesandsevenattacktypes,includingdataset [24], collected at Singapore University of Technology from a water treatment system, consisting of 449,920 samples. In this dataset, 87.9% and 12.1% were normal and attack samples, respectively. Each dataset sample was formed by 51 features that were the physical measurements of the systems. In addition, this dataset consisted of 31 different attack scenarios that could be used for attack attribution.

5.CONCLUSION

This paper proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS data. The attack detection stage uses deep representation learning to map the samples to new higher dimensional space and applies

a DT to detect the attack samples. This stage is robust to imbalanced datasets and capable of detecting previously unseen attacks. The attack attribution stage is an ensembles of several one-vs-all classifierseach trained on a specific attack attribute. The entire model forms a complex DNN with a partially connected and fully connected component that can accurately attribute cyberattacks, as demonstrated. Despite the complex architecture of the proposed framework, the computational complexity of the training and testing phases are respectively O(n4) and O(n2), (n is the number of training samples), which are similar to those of other DNN-based techniques in the literature. Moreover, the proposed framework can detect and attribute the samples timely with a better recall and f-measure than previous works. Future extension includes the design of a cyber-threat hunting component to facilitate the identification of anomalies invisible to the detection component for example by building a normal profile over the entire system and theassets.

6. REFERENCES

[1] https://www.kaggle.com/c/challenges-inrepresentation-learning-faciaL-expressionrecognition-challenge/data, 2003.

[2] Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.D.Baswaraj, J.Greeda 2019 “Improved Migration Performance In Virtualized Cloud Datacenters” International Journal of Scientific & Technology Research. Volume 8, Issue 09,page no.1515-1518 September 2019. (Scopus indexed).

[3] Krizhevsky, Alex, Ilya Sutskever, and GeoffreyE. Hinton. ”Imagenet classification with deep convolutionalneural networks.” Advances in neuralinformation processing systems. 2012.

[4] Annadi Jahnavi, Hanumandla Bhavana, Dr. R. Jegadeesan “An Implementation of Detecting Password Pattern In Dictionary Attack” International Journal of Advanced Science and technology. ISSN 2005-42386, Page no: 84-92 July,2019.

[5] A. Mollahosseini, D. Chan, and M. H. Mahoor, “Going Deeper inFacial Expression Recognition using Deep Neural Networks,” CoRR,vol. 1511, 2015.

[6] Pramerdorfer, C., Kampel, M.: Facial expression recognition usingconvolutional neural networks: state of the art. PreprintarXiv:1612.02903v1, 2016.

[7]Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.C.N.Ravi, J.Greeda2019 “A Secure Transaction Authentication Scheme using Blockchain based on IOT” International Journal of Scientific & Technology Research. VOLUME 8, ISSUE 10,Page no:2217-2221 OCTOBER 2019. ISSN 2277-8616.

[8] Quinn M., Sivesind G., and Reis G., "Real-time Emotion RecognitionFrom Facial Expressions", 2017.

[9] Dr R Jegadeesan, Dr.C.N.Ravi, Dr.A.Nirmal Kumar 2020 "Automatic Rice Quality Detection Using Morphological and Edge Detection Techniques" ICCCE 2020 3rd International Conference on Communications and cyber Physical Engineering, Metadata of the chapter that will be visualized in Springer Link. Volume, issue, May.2020 Page No.233-242, Springer conference..

[10] Wang J., and Mbuthia M., "FaceNet: Facial Expression RecognitionBased on Deep Convolutional Neural Network", 2018.

[11] P.Sandhya, Mogili Ravindar, Dr.M.Sujatha, Dr R Jegadeesan, 2020 "DISCOVERY OF INFORMATION DISSEMINATORS AND DIFFUSION PROCESS IN ONLINE SOCIAL NETWORKS" Alochana Chakra Journal, Volume IX, Issue VII, July/2020, ISSN NO:2231-3990,Page No:747-752.

[12] Minaee S., Abdolrashidi A., "Deep-Emotion: Facial ExpressionRecognition Using Attentional Convolutional Network", 2019.

[13]. Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.D.Baswaraj, J.Greeda 2019 "Improved Migration Performance In Virtualized Cloud Datacenters" International Journal of Scientific & Technology Research. Volume 8, Issue 09,page no.1515-1518 September 2019. **(Scopus indexed)**

[14].Annadi Jahnavi, Hanumandla Bhavana, Dr. R. Jegadeesan "An Implementation of Detecting Password Pattern In Dictionary Attack" International Journal of Advanced Science and technology. ISSN 2005-42386, Page no: 84-92 July,2019(Indexed by Scopus, Elsevier).

[16].Dr.A.Nirmal Kumar, Dr.R.Jegadeesan, Dr.C.N.Ravi, J.Greeda2019 "A Secure Transaction Authentication Scheme using Blockchain based on IOT" International Journal of Scientific & Technology Research. VOLUME 8, ISSUE 10,Page no:2217-2221 OCTOBER 2019. ISSN 2277-8616 (Scopus indexed)

[17].Dr R Jegadeesan, Dr.C.N.Ravi, Dr.A.Nirmal Kumar 2020 "Automatic Rice Quality Detection Using Morphological and Edge Detection Techniques" ICCCE 2020 3rd International Conference on Communications and cyber Physical Engineering, Metadata of the chapter that will be visualized in Springer Link. Volume, issue, May.2020 Page No.233-242, Springer conference.