DETECTION AND ATTRIBUTION OF CYBER ATTACKS IN IOT ENABLED CYBER PHYSICAL SYSTEM.

Mr B.S Murthy [1], I. Mary Sujatha [2],

[1]**Assistant professor , MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- suryanarayanamurthy.b@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:- sujathairrinki@gmail.com

ABSTRACT

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 decision 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.

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. BlackEnergy3 was another campaign that targeted Ukraine power grids in 2015, resulting in power outage that affected approximately 230,000 people

2 RELEATED WORK

A literature survey for Detecting attribution of Cyber-attacks in IoT enabled Cyber physical system has revolutionized various sectors, including smart grids, healthcare, and industrial automation. However, this integration also increases the attack surface for cyber threats. The detection and attribution of cyber-attacks in IoT-enabled CPS are critical for maintaining security, reliability valuable insights into existing research and help identify gaps in the field. Here's a brief overview of the key areas and topics you should consider including in your literature survey

3 IMPLEMENTATION STUDY

Existing System:

The comparative summary suggested that the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best algorithm, with a recall of 0.8718; and the LR is the worst- performing algorithm, with a recall of 0.4744. The authors also reported that the ANN could not detect 12.82% of the attacks and considered 0.03% of the normal samples to be attacks. In addition, LR, SVM, and KNN considered many attack samples as normal samples, and these ML algorithms are sensitive to imbalanced data. In other words, they are not suitable for attack detection in ICS.

Disadvantages:

1) The system is implemented by Conventional Machine Learning.

2) The system doesn’t implement Conventional Machine Learning method**.**

Proposed System & alogirtham

The proposed attack detection consists of two phases, namely representation learning and detection phase. Using a conventional unsupervised DNN on an imbalanced dataset yielded a DNN model that mainly learned majority class patterns and missed minority class characteristics. Most researchers have tried to address this challenge by generating new samples or removing certain samples to make the dataset balanced and then passing the data to a DNN. However, in ICS/IIoT security applications, generating or removing samples are not reasonable solutions.

4.1 Advantages:

1) The proposed two-phase attack detection component has been implemented.

2) Unsupervised models that incorporate process/physical data can complement a system’s monitoring since they do not rely on detailed knowledge of the cyber-threats.

4 IMLEMENTATION

4.1 MODULES

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.

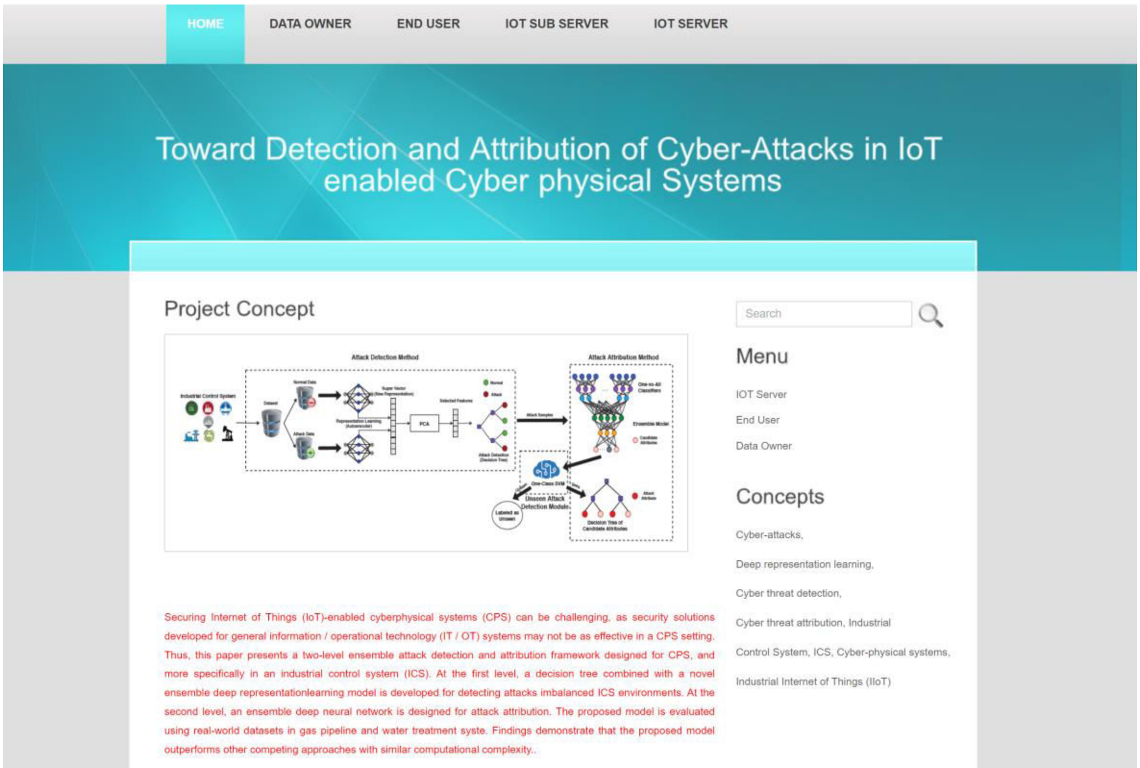
User: The user is divided into two categories. One is the initial user who uploads files that did not exist in the cloud previously. The other one is the subsequent users who upload files that the IOT Sub Server kept. The initial user generates the authenticators for each encrypted file, then uploads 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.

IOT Sub Server: The IOT SUB SERVER is responsible for helping users generate the file index and the file label with his private key. With the file index, the cloud can verify whether the file uploaded by the user is duplicated or not. With the file label, the user can generate some keys for encryption and authenticator generation.

5 RESULTS AND DISCUSSION

SCREEN SHOTS

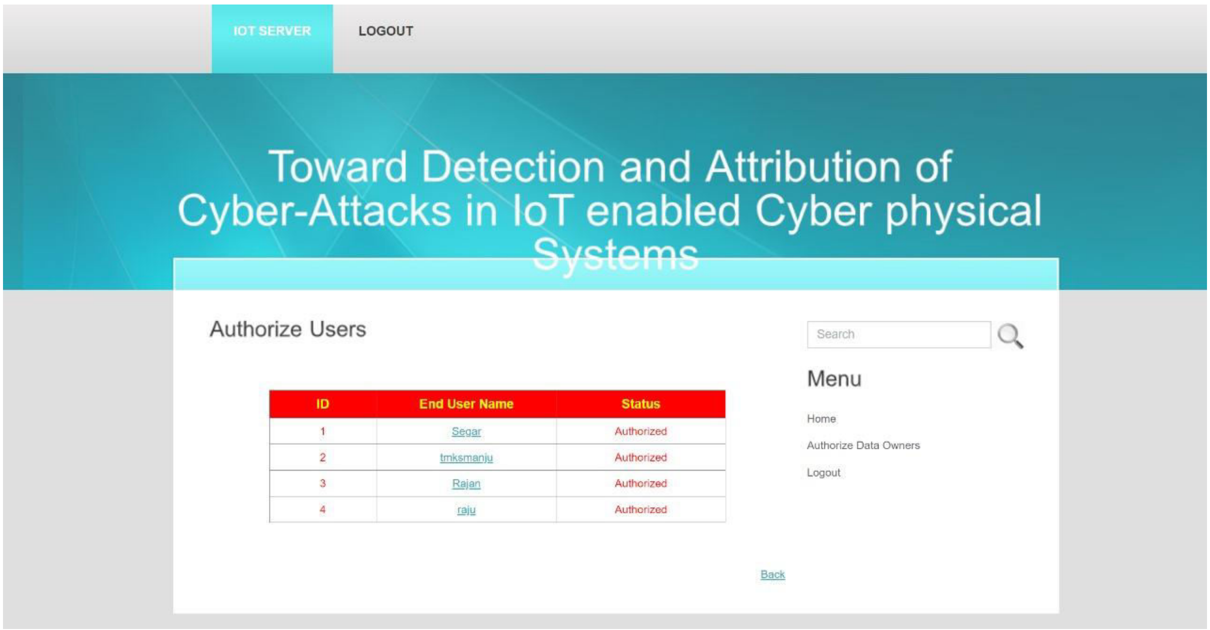
5.2.1 Home Page


HOME
DATA OWNER
END USER
IOT SUB SERVER
IOT SERVER
Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems
Project Concept
Attack Detection Method
Attack Attribution Method
Industrial Control System
PCA
Unseen Attack Detection Module
One-Class SVM
Labeled as Unseen
Decision Tree of Candidate Attributes
Search
Menu
IOT Server
End User
Data Owner
Concepts
Cyber-attacks,
Deep representation leaming,
Cyber threat detection,
Cyber threat attribution, Industrial
Control System, ICS, Cyber-physical systems,
Industrial Internet of Things (IIoT)

Securing Internet of Things (IoT)-enabled cyberphysical 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 decision tree combined with a novel ensemble deep representationlearning 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 syste. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity..

FIG 5.1 Home Page with Project Concept – SCREEN SHOT

5.2.2 IoT Server Page



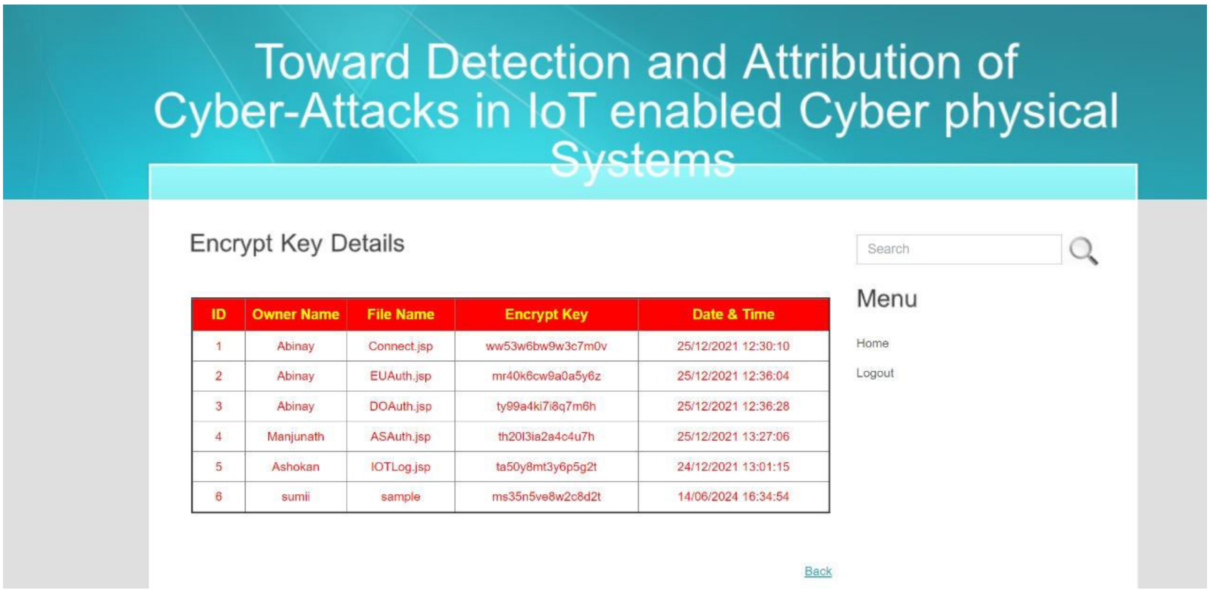
Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems

Authorize Users

ID	End User Name	Status
1	Segar	Authorized
2	tmksmanju	Authorized
3	Rajan	Authorized
4	raju	Authorized

FIG 5.2 IoT Server – SCREEN SHOT

5.2.3 Encrypt Key Details



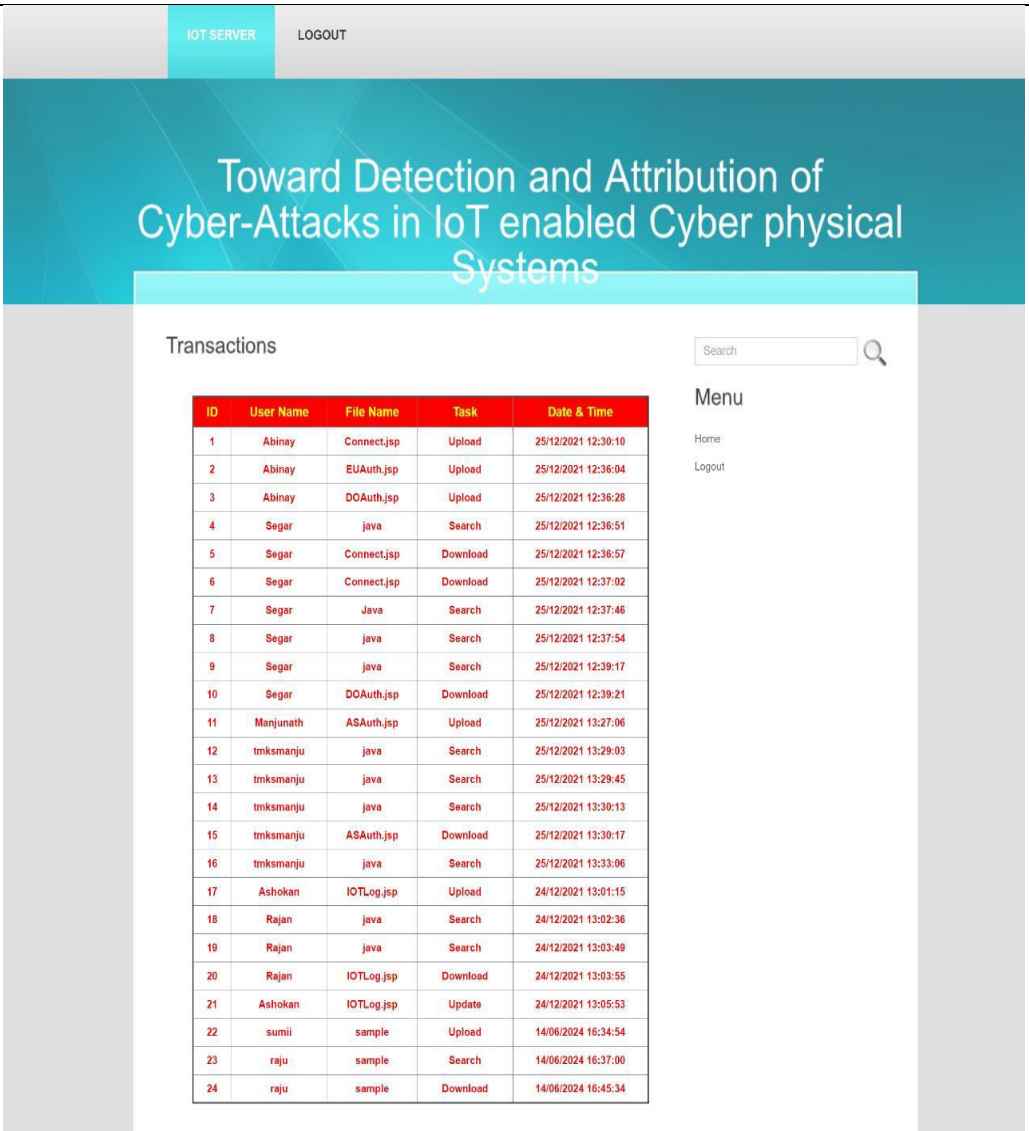
Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems

Encrypt Key Details

ID	Owner Name	File Name	Encrypt Key	Date & Time
1	Abinay	Connect.jsp	ww53w6bw9w3c7m0v	25/12/2021 12:30:10
2	Abinay	EUAuth.jsp	mr40k6cw9a0a5y6z	25/12/2021 12:36:04
3	Abinay	DOAuth.jsp	ty99a4ki7i8q7m6h	25/12/2021 12:36:28
4	Manjunath	ASAuth.jsp	th20l3ia2a4c4u7h	25/12/2021 13:27:06
5	Ashokan	IOTLog.jsp	ta50y8mt3y6p5g2t	24/12/2021 13:01:15
6	sumii	sample	ms35n5ve8w2c8d2t	14/06/2024 16:34:54

FIG 5.3 Encrypt Key – SCREEN SHOT

5.2.4 IOT Server transcations

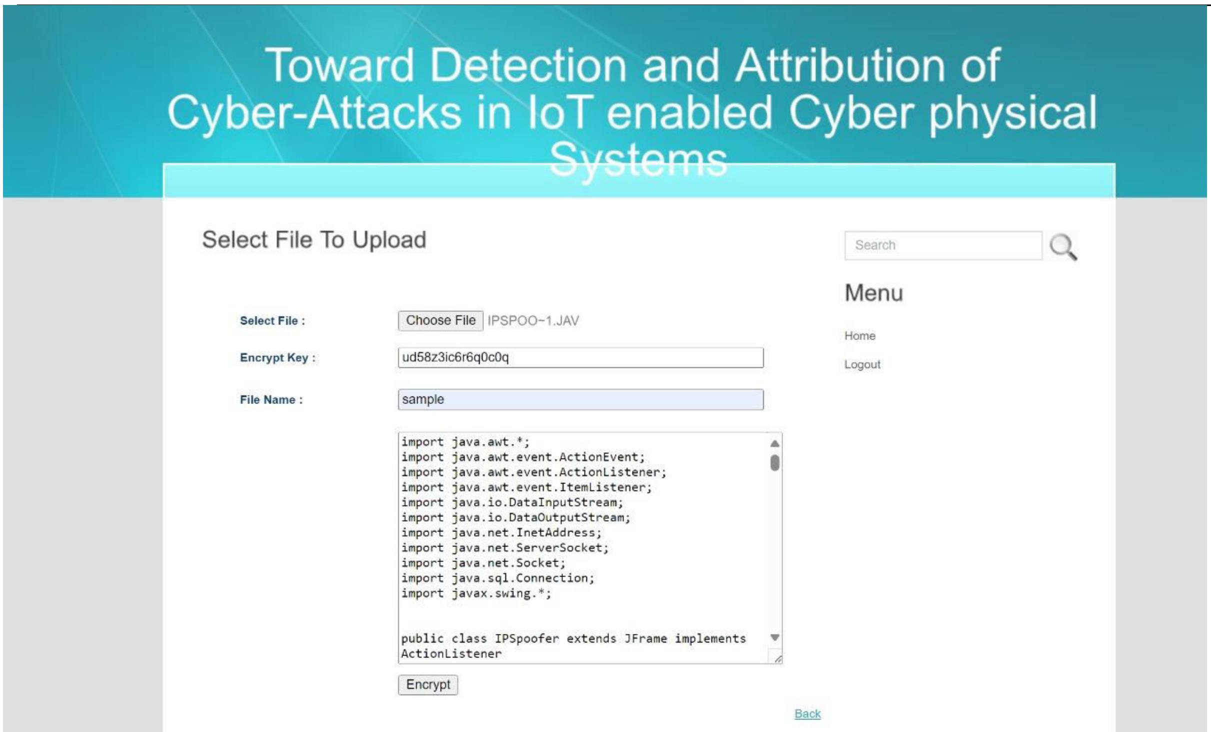

IOT SERVER
LOGOUT
Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems
Search
Menu
Home
Logout

Transactions

ID	User Name	File Name	Task	Date & Time
1	Abinay	Connect.jsp	Upload	25/12/2021 12:30:10
2	Abinay	EUAuth.jsp	Upload	25/12/2021 12:36:04
3	Abinay	DOAuth.jsp	Upload	25/12/2021 12:36:28
4	Segar	java	Search	25/12/2021 12:36:51
5	Segar	Connect.jsp	Download	25/12/2021 12:36:57
6	Segar	Connect.jsp	Download	25/12/2021 12:37:02
7	Segar	Java	Search	25/12/2021 12:37:46
8	Segar	java	Search	25/12/2021 12:37:54
9	Segar	java	Search	25/12/2021 12:39:17
10	Segar	DOAuth.jsp	Download	25/12/2021 12:39:21
11	Manjunath	ASAuth.jsp	Upload	25/12/2021 13:27:06
12	tmksmanju	java	Search	25/12/2021 13:29:03
13	tmksmanju	java	Search	25/12/2021 13:29:45
14	tmksmanju	java	Search	25/12/2021 13:30:13
15	tmksmanju	ASAuth.jsp	Download	25/12/2021 13:30:17
16	tmksmanju	java	Search	25/12/2021 13:33:06
17	Ashokan	IOTLog.jsp	Upload	24/12/2021 13:01:15
18	Rajan	java	Search	24/12/2021 13:02:36
19	Rajan	java	Search	24/12/2021 13:03:49
20	Rajan	IOTLog.jsp	Download	24/12/2021 13:03:55
21	Ashokan	IOTLog.jsp	Update	24/12/2021 13:05:53
22	sumii	sample	Upload	14/06/2024 16:34:54
23	raju	sample	Search	14/06/2024 16:37:00
24	raju	sample	Download	14/06/2024 16:45:34

FIG 5.4 IoT Server Transaction – SCREEN SHOT

5.2.5 Screen that shows files to upload



Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems
Search
Menu
Home
Logout
Choose File
Encrypt
Back

Select File To Upload

Select File : IPSPOO~1.JAV

Encrypt Key : ud58z3ic6r6q0c0q

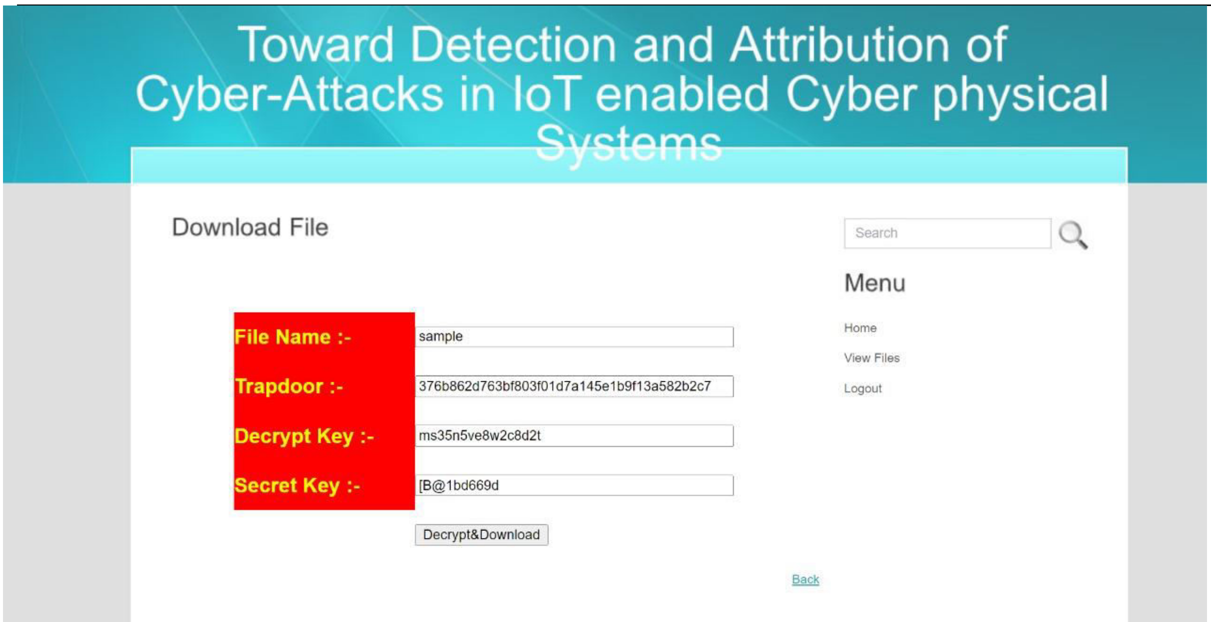
File Name : sample

```
import java.awt.*;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.ItemListener;
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.net.InetAddress;
import java.net.ServerSocket;
import java.net.Socket;
import java.sql.Connection;
import javax.swing.*;


public class IPSpoofer extends JFrame implements
ActionListener
```

FIG 5.5 Files To Upload – SCREEN SHOT

5.2.6 Download file screen



Toward Detection and Attribution of Cyber-Attacks in IoT enabled Cyber physical Systems

Download File

File Name :- sample

Trapdoor :- 376b862d763bf803f01d7a145e1b9f13a582b2c7

Decrypt Key :- ms35n5ve8w2c8d2t

Secret Key :- [B@1bd669d

FIG 5.6 Download File – SCREEN SHOT

6. CONCLUSION AND FUTURE WORK

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 the 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 ensemble of several one-vs-all classifiers, each 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 the assets.

7. REFRENCES

[1] F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble,
“Multilayer Data-Driven Cyber-Attack Detection System for Industrial
Control Systems Based on Network, System, and Process Data,” IEEE
Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369,

2019.

[2] R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, “Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber-Physical System,” IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, 2019.

[3] E. Nakashima, “Foreign hackers targeted U.S. water plant in apparent malicious cyber attack, expert says.” [Online]. Available: https://www.washingtonpost.com/blogs/checkpointwashington/ post/foreign-hackers-broke-into-illinois-water-plant-controlsystem-industry-expert-says/2011/11/18/gIQAgmTZYN blog.html

[4] G. Falco, C. Caldera, and H. Shrobe, “IIoT Cybersecurity Risk Modeling for SCADA Systems,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486–4495, 2018.

[5] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, “Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems,” IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, 2018.

[6] S. Ponomarev and T. Atkison, “Industrial control system network intrusion detection by telemetry analysis,” IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, 2016.

[7] J. F. Clemente, “No cyber security for critical energy infrastructure,” Ph.D. dissertation, Naval Postgraduate School, 2018.

[8] C. Bellinger, S. Sharma, and N. Japkowicz, “One-class versus binary classification: Which and when?” in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.

[9] I. Goodfellow, Y. Bengio, and A. Courville, Deep learning. MIT Press, 2016. [Online]. Available: http://www.deeplearningbook.org