REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
03-10-2022	Final Report	10-May-2021 - 9-Feb-2022

4. TITLE AND SUBTITLE

Final Report: COVERT ID: Cybersecurity Operations Vectors: Verifying External Resilience of Transgressors and their Identification through Cybersecurity Forensics

5a. CONTRACT NUMBER
W911NF-21-1-0201

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

Florida International University
10555 West Flagler, EC 2441

Miami, FL 33174 -1630

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
78628-NC-II.5

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sundararaj Iyengar
UU	UU	UU	UU		19b. TELEPHONE NUMBER 305-348-3947

RPPR Final Report
as of 15-Dec-2022

Agency Code: 21XD

Proposal Number: 78628NCII **Agreement Number: W911NF-21-1-0201**
INVESTIGATOR(S):

Name: Sundararaj Iyengar
Email: sundararaj.iyengar@fiu.edu
Phone Number: 3053483947
Principal: Y

Organization: **Florida International University**
Address: 10555 West Flagler, EC 2441, Miami, FL 331741630
Country: USA
DUNS Number: 071298814 EIN: 756000121

Report Date: 09-May-2022 Date Received: 03-Oct-2022
Final Report for Period Beginning 10-May-2021 and Ending 09-Feb-2022

Title: COVERT ID: Cybersecurity Operations Vectors: Verifying External Resilience of Transgressors and their Identification through Cybersecurity Forensics
Begin Performance Period: 10-May-2021 **End Performance Period:** 09-Feb-2022
Report Term: 0-Other

Submitted By: Jerry Miller Email: Jerry.Miller@fiu.edu
Phone: (305) 348-7984

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 0 **STEM Participants:** 4

Major Goals: The proposed research will develop COVERT ID: A Forensic suite of software tools to Identify Cybersecurity attack Operations Vectors, while Verifying External Relationships of Transgressors and their Identifications. This new research effort will consists of four components, namely: 1) robust, resilient malware identification agents, 2) rapid forensic analysis of identifying features, 3) employment of artificial intelligence and machine learning components, and, 4) near-real-time identification, verification and mapping of vectors and clusters associated with the malicious operators.
Methods to be Employed:
The research will introduce novel techniques in machine learning for building deep packet inspection (DPI) capabilities by adopting Ensemble Learning, which is the use multiple learning algorithms to obtain better predictive performance in targeting high rates of precision identification of IoT attackers and their malware.

Accomplishments: Result 1: AI Powered Threat Prediction and Protection Algorithmic Framework
This work presents an Artificial Intelligence powered Threat Prediction and Protection (TPP) Algorithmic Framework to predict the cyber security attacks using correlational neural networks.
Latesh Kumar KJ, Yashas Hariprasad, Naveen Kumar Chaudhary. “AI Powered Correlation Technique to detect Virtual Machine Attacks in Private Cloud Environment”,; To appear as a Book-Chapter in a forthcoming book Titled: “AI Embedded Assurance for Cyber System”, Cliff Wang, S. S. Iyengar, Kun Sun, Springer Nature (January 2023)

Summary of the work is as follows:
“The efficacy of cyber forensic systems primarily depends on the real-time discovery and the analysis of the threats in a timely manner. This process requires the development of smart techniques with good precession, accuracy and also should provide an insight to the details about the cyber-attacks. This paper addresses the above concerns by presenting a novel AI powered Threat Prediction and Protection (TPP) algorithm based on Correlational Recurrent Neural Network (Corrnet) technique to predict cyber-attacks in a private cloud environment containing financial data. More specifically, the AI based foundational techniques proposed in the paper, correlates efficiently multi-dimensional data such as IP address, Source Port, Destination port, Source IP, date and time etc. generated during the attack process of investigation. The implementation of the proposed algorithm in a test-bed environment is very encouraging and provides 92.5% precision and accuracy in predicting the cyber-attacks in an un-structured environment.”

Result 2: Cyber Security Attack Detection Framework for Control Message Flooding in an IoT Network

RPPR Final Report
as of 15-Dec-2022

This work addresses the availability issues in the IoT Communications network systems and also presents an attack detection algorithmic framework for the DDoS traffic by IoT Devices.
Cyber Security Attack Detection Framework for DODAG Control Message Flooding in an IoT Network,; Jerry Miller, Lawrence Egharevba, Yashas Hariprasad, Latesh Kumar K J, Naveen Kumar Chaudhary, International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022).; Springer Nature; Lecture Notes in Electrical Engineering Series (2022) (Under Review)

Summary of the work is as follows:
“Advancement in the IoT technologies and the futuristic device’s usage influences the human life in all the aspects of day to day activities. Moreover, human reliance on smart objects makes IoT an important tool. IoT network enables the communication among the smart devices by embedding software, sensors etc. which makes an object smart and intelligent. Though it offers many advantages, it is a matter of concern in protecting the privacy, integrity, and availability of the users’ data, and these issues need to be addressed in the implementation of the devices before it turns out to be a threat. DDoS is one such security threat which can bring down the resource constrained IoT network. In this work, we have tried to address the existing availability issues in the IoT communication network and based on the analysis, proposed an attack detection framework for the DDoS traffic generated by IoT devices. The attack detection is done by keeping track of the usage of IoT devices parameter like power consumption, bandwidth, and monitoring the IoT network traffic to oversee the number of messages exchanged between the nodes as part of the RPL DODAG construction. So that resources and bandwidth can be used for genuine communication. The proposed work has achieved better bandwidth and our simulation framework obtained good results in identifying DDoS attacks.”

Training Opportunities: Under the tutelage of Dr. S.S. Iyengar the following junior Ph.D. Post Doc and students were trained in Artificial intelligence and digital forensics. The students were co-authors in research publications under this grant.
Latesh Kumar KJ (Post Doctoral Fellow)
PhD students:Yashas Hariprasad, Naveen Kumar Chaudhary, Jerry Miller
M.S. Students: Lawrence Egharevba

Researchers submitted a forthcoming publication to International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022).

Results Dissemination: Research results were disseminated through a conference paper and a book chapter as outlined in the following:
Cyber Security Attack Detection Framework for DODAG Control Message Flooding in an IoT Network,; Jerry Miller, Lawrence Egharevba, Yashas Hariprasad, Latesh Kumar K J, Naveen Kumar Chaudhary, International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022).; Springer Nature; Lecture Notes in Electrical Engineering Series (2022) (Under Review)
Latesh Kumar KJ, Yashas Hariprasad, Naveen Kumar Chaudhary. “AI Powered Correlation Technique to detect Virtual Machine Attacks in Private Cloud Environment”,; To appear as a Book-Chapter in a forthcoming book Titled: “AI Embedded Assurance for Cyber System”, Cliff Wang, S. S. Iyengar, Kun Sun, Springer Nature (January 2023)

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: Postdoctoral (scholar, fellow or other postdoctoral position)
Participant: Latesh K.J. Kumar
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Jerry Franklin Miller
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Yashas Hariprasad
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Lawrence Egharevba
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: PD/PI
Participant: Sitharama S. Iyengar
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 4-Under Review
Conference Name: International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022)
Date Received: 01-Oct-2022 Conference Date: 02-Dec-2022 Date Published:
Conference Location: Kurti, Ponda, Goa 403512 India
Paper Title: Cyber Security Attack Detection Framework for DODAG Control Message Flooding in an IoT Network
Authors: Jerry Miller, Lawrence Egharevba, Yashas Hariprasad, Latesh Kumar K J, Naveen Kumar Chaudhary
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 15-Dec-2022

Publication Type: Conference Paper or Presentation **Publication Status:** 4-Under Review
Conference Name: International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022)
Date Received: 03-Oct-2022 Conference Date: 02-Dec-2022 Date Published:
Conference Location: Ponda, Goa, India
Paper Title: Lightweight Malicious Packet Classifier for IoT Networks
Authors: Seyedsina Nabavirazavi, S. Sitharama Iyengar, Naveen Kumar Chaudhary
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 0-Other
Conference Name: International Conference on Information Security, Privacy and Digital Forensics (ICISPD 2022)
Date Received: 03-Oct-2022 Conference Date: 02-Dec-2022 Date Published:
Conference Location: Ponda, Goa, India
Paper Title: Boundary Based Fake Face Anomaly Detection in Videos using Recurrent Neural Networks
Authors: Yashas Hariprasad, Latesh Kumar K. J., Suraj L., and S. Sitharama Iyengar
Acknowledged Federal Support: **Y**

Partners
Dr. Naveen Kumar Chaudhary
Gandhinagar, IND
4
Dr. Naveen Kumar Chaudhary is a research collaborator and faculty member of the National Forensic Science University. He provided assistance in research mentoring for students and contributed to publications under this grant as a volunteer research collaborator.

I certify that the information in the report is complete and accurate:
Signature: Jerry F. Miller
Signature Date: 10/3/22 9:58AM

Final Technical Report

W911NF2110201 / 78628-N-CII

Project Title: COVERT ID: Cybersecurity Operations Vectors: Verifying External Resilience of Transgressors and their Identification through Cybersecurity Forensics

Result 1: AI Powered Threat Prediction and Protection Algorithmic Framework

This work presents an Artificial Intelligence powered Threat Prediction and Protection (TPP) Algorithmic Framework to predict the cyber security attacks using correlational neural networks.

Latesh Kumar KJ, Yashas Hariprasad, Naveen Kumar Chaudhary. "AI Powered Correlation Technique to detect Virtual Machine Attacks in Private Cloud Environment",; To appear as a Book-Chapter in a forthcoming book Titled: "AI Embedded Assurance for Cyber System", Cliff Wang, S. S. Iyengar, Kun Sun, Springer Nature (January 2023)

Summary of the work is as follows:

"The efficacy of cyber forensic systems primarily depends on the real-time discovery and the analysis of the threats in a timely manner. This process requires the development of smart techniques with good precession, accuracy and also should provide an insight to the details about the cyber-attacks. This paper addresses the above concerns by presenting a novel AI powered Threat Prediction and Protection (TPP) algorithm based on Correlational Recurrent Neural Network (Corrnet) technique to predict cyber-attacks in a private cloud environment containing financial data. More specifically, the AI based foundational techniques proposed in the paper, correlates efficiently multi-dimensional data such as IP address, Source Port, Destination port, Source IP, date and time etc. generated during the attack process of investigation. The implementation of the proposed algorithm in a test-bed environment is very encouraging and provides 92.5% precision and accuracy in predicting the cyber-attacks in an un-structured environment."

Result 2: Cyber Security Attack Detection Framework for Control Message Flooding in an IoT Network

This work addresses the availability issues in the IoT Communications network systems and also presents an attack detection algorithmic framework for the DDoS traffic by IoT Devices.

Cyber Security Attack Detection Framework for DODAG Control Message Flooding in an IoT Network,; Jerry Miller, Lawrence Egharevba, Yashas Hariprasad, Latesh Kumar K J, Naveen Kumar Chaudhary, International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022).; Springer Nature; Lecture Notes in Electrical Engineering Series (2022) (Under Review)

Summary of the work is as follows:

"Advancement in the IoT technologies and the futuristic device's usage influences the human life in all the aspects of day to day activities. Moreover, human reliance on smart objects makes IoT an important tool. IoT network enables the communication among the smart devices by embedding software, sensors etc. which makes an object smart and intelligent. Though it offers many advantages, it is a matter of concern in protecting the privacy, integrity, and availability of the users' data, and these issues need to be addressed in the implementation of the devices before it turns out to be a threat. DDoS is one such security threat which can bring down the resource constrained IoT network. In this work, we have tried to address the existing availability issues in the IoT communication network and based on the analysis, proposed an attack detection framework for the DDoS traffic generated by IoT devices. The attack detection is done by keeping track of the usage of IoT devices parameter like power consumption, bandwidth, and monitoring the IoT network traffic to oversee the number of messages exchanged between the nodes as part of the RPL DODAG construction. So that resources and bandwidth can be used for genuine communication. The proposed work has achieved better bandwidth and our simulation framework obtained good results in identifying DDoS attacks."

Other Related Works:

1. Hariprasad, Y., Latesh Kumar, K. J., Suraj, L., & Iyengar, S. S. (2022). Boundary-Based Fake Face Anomaly Detection in Videos Using Recurrent Neural Networks. In Proceedings of SAI Intelligent Systems Conference (pp. 155-169). Springer Nature; "Lecture Notes in Networks and Systems.

2. Seyedsina Nabavirazavi, S. Sitharama Iyengar and Naveen Kumar Chaudhary; Lightweight Malicious Packet Classifier for IoT Networks;, International Conference on Information Security, Privacy, and Digital Forensics (ICISPD 2022).; Springer Nature Lecture Notes in Electrical Engineering Series (2022) (Under Review)