

2019 International Conference on Cybersecurity (ICoCSec 2019)

**Negeri Sembilan, Malaysia
25-26 September 2019**



IEEE Catalog Number: CFP19V57-POD
ISBN: 978-1-7281-5658-3

**Copyright © 2019 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP19V57-POD
ISBN (Print-On-Demand):	978-1-7281-5658-3
ISBN (Online):	978-1-7281-5657-6

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

NO	PAPER TITLE	PAGES
1	FEATURE EXTRACTION AND SELECTION METHOD OF CYBER-ATTACK AND THREAT PROFILING IN CYBERSECURITY AUDIT	1 – 6
2	USING ATTACK PATTERN FOR CYBER ATTACK ATTRIBUTION	7 - 12
3	THE PRIMARILY STUDY OF ELECTRONIC RECORDS MANAGEMENT SYSTEM (ERMS) FOR YEMEN OIL AND GAS CORPORATION (YOGC) SUBSIDIARIES	13 - 19
4	ON THE ANALYSIS OF THE IMPACT OF SCHEDULING PLANS IN SAFETY CRITICAL REQUIREMENTS IN VIRTUALIZATION	20 - 25
5	SPEAR PHISHING SIMULATION IN CRITICAL SECTOR (TELECOMMUNICATION AND DEFENCE SUB-SECTOR)	26 - 31
6	USING TEXT ANNOTATION TOOL ON CYBER SECURITY NEWS - A REVIEW	32 - 36
7	A THEORETICAL REVIEW: RISK MITIGATION THROUGH TRUSTED HUMAN FRAMEWORK FOR INSIDER THREATS	37 - 42
8	REVIEW OF DIGITAL WALLET REQUIREMENTS	43 - 48
9	INSTRUMENTING API HOOKING FOR A REALTIME DYNAMIC ANALYSIS	49 - 52
10	UNINTENTIONAL INSIDER THREATS COUNTERMEASURE S MODEL (UITCM)	53 - 58
11	A QOS APPROACH FOR INTERNET OF THINGS (IOT) ENVIRONMENT USING MQTTA PROTOCOL	59 - 63
12	FRAMEWORK DESIGN FOR SECURED LOCAL CLOUD DATA QUERY PROCESSING ANALYSIS	64 - 69
13	MOBILE MALWARE CLASSIFICATION FOR SOCIAL MEDIA APPLICATION	70 - 75
14	TAGRAPH: KNOWLEDGE GRAPH OF THREAT ACTOR	76 - 80
15	CRIME IN VIRTUAL REALITY: DISCUSSION	81 - 85
16	RANSOMWARE ENTITIES CLASSIFICATION WITH SUPERVISED LEARNING FOR INFORMAL TEXT	86 - 90
17	INTRUSION DETECTION SYSTEM TO ENHANCE NETWORK SECURITY USING RASPBERRY PI HONEYPOT IN KALI LINUX	91 - 95