Back Propogation Neural Network based Cybersecurity Information Retrival from Repository

Ahmed Aweidah Hamad Alosaimi[a] and Mourad Elloumi[b]
[a] Masters students, Faculty of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia
[b]Professor, Faculty of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: The wireless network is interconnected with pervasiveness of vast range of personal devices. The advancement of technological devices involved in generation, processing, exchange, sharing and utilization of specific applications. Thus, cyberspace has been adopted for device security for business, organization and government. To retain cybersecurity machine learning (ML) is employed for detection and authentication of malware. However, ML attacks are vulnerable for both training and testing phases for reduction of security breaches. This paper developed an appropriate cybersecurity mechanism for repositories for data exchange. The proposed scheme involved in definition of data model with Incident Object Description Exchange structured information format. The structured information is utilized in XML format of cybersecurity for information exchange. The developed structured information utilizes ML for analysis of feasibility and usability. The simulation analysis demonstrated that proposed ML exhibits significant performance for cybersecurity estimation.

Keywords: Cybersecurity, Structured Information, Machine Learning, Incident Object Description Exchange Format (IODEF), XML

1. Introduction

In recent years, cybersecurity has been interested in everyone with data storage and safety, personal computer malware defense, safe financial services and the democratic elections, both influenced by a growth in the processing of big data and the advancement made in ML [1]. In all sectors, AI has been integrated into information systems and AI vulnerability reports and cybersecurity concerns have risen at the same time [2]. By 2021, 75% of all company applications are expected to use any ML-based AI, which enhances their cybersecurity significance [3]. AI machine errors are not just worrying, as AI has been using ML for defensive purposes [4]. ML is also willing, as a possible tool, to arm otherwise unusable data. AI has defensive potential, on the other hand, such as being able to anticipate and deter malicious activities[5]. Existing solutions do not make other cybersecurity initiatives redundant, considering the rising presence of AI in cybersecurity. Every day, the number of cyber-attacks is rising. To effectively preserve cybersecurity, a company needs to share cybersecurity data with others, including outside its borders. However, such exchanges are most commonly carried out by individual operators based on their networks and are typically carried out using manual operations emails Telephone calls and face-to-face meetings, which take a substantial amount of time[6], for example. More delay causes further harm to victims in an incident response process. IODEF [7] was implemented to deal with this problem. It defines a data model and its XML schemes to explain event information and enables information to be shared between computers. Several organizations, such as US-CERT, have already used it and have advanced the electronic sharing of information. However, a lack of manpower resources is exacerbated by the enhanced number of cyber-incidents. Since their education takes time, it is difficult to dramatically or quickly increase the number of skilled operators[8].Security activities are also supposed to be simplified by using IT to carry out some of human operators' workload. From this perspective, IODEF has an excessive number of free-text fields that can not be automatically understood by computers, A more structured structure of the data is needed [9]. The concept of a universal data structure that can be used for different security operations is a simple solution to this problem, but the necessary data structure varies depending on operations, and these can change in future[10]. Machine-readable and -processable are IODEF-SCI documents that contain embedded structured documents [11]. It is utilized for cybersecurity operations on receiver side and can speed up automation of cybersecurity operations. Those vulnerabilities that have been utilized must be reported by an organization that wishes to report a security event [12]. Sender may then use IODEF-SCI guide, in which an XML-based pattern of attack is implemented using syntax and terminology defined by an industry-standard, rather than describing all details in free text format [13]. The recipient will also collect certain archives of attack trends in his files and, if appropriate, circulate them to interested parties without need for human interference. Another example is the potential for a manager to send a questionnaire to host computers while they are installed to verify the host machine configuration in their organization. The query can be automatically generated with XML-based configure information after query is obtained and can then be inserted in an IODEF document, and returned to IODEF-STIC. In the current study, cybersecurity analysis using machine learning is presented with consideration of IODEF format. The analysis is based on the consideration of structured information for information exchange. Data structure is based on industrial

applications with dynamic information exchange. Here, IODEF is involved in dynamic specification of attacks in the network for improved cybersecurity for estimation. The developed ML utilizes Back Propagation Neural Network (BPNN) for estimation of information for preventing cybersecurity.

2. Related Works

In this section, existing literature conducted for estimation of information for cybersecurity is presented. In [15] outlines several suggestions for successful data sharing between Certificates but uses protected messaging mechanisms as PGP as the solution preferential by the authors. While this is an easy option for privacy and confidence, sharing vast volumes of data is tedious. Furthermore, when the attack is over, it cannot withdraw entry. Another work[16] known as drop [for Forensics Dropbox] provides a social network architecture based on the XMPP and behavior stream specifications that allow users to post malware information on the networks. However, this is limited in particular to not sensitive information to avoid confidence and privacy concerns from being discussed. The core concepts of cybersecurity were suggested as follows: vulnerabilities, risks and assaults, safeguards, protocols, countermeasures, defensive policies and mechanisms [17]. This list was further expanded in [18], including data security and criticality principles. There are also other categorizations, as in[19] AI in the area of cybersecurity is grouped into 16 types, some of which can also be further separated. Also, 11 cybersecurity sub-categories were addressed that have influenced ML applications: protection of networks, endpoint, server, IoT and internet security, event and security operations, threatened intelligence, mobile security, cloud security, identity and access control, and human security and network security. In these previous research and categorizations, AI and ML were not directly taken into consideration, even though associated principles like data protection and critique were discussed. Due to increasing involvement of AI in cybersecurity, educators need to consider in what directions and what kinds of AI technologies can be used in their teaching. Recently, academics have proposed that computer security education should be funded by industry staff to ensure that students have access to up-to-date information[21]. This idea has already been applied with several businesses joining universities to build wide open online courses (MOOC) on AI or to develop stand-alone online courses. A company named Reaktor partnered with University of Helsinki to build a free course called Elements of AI which will show you how to use their Tensor Flow APIs. For example Google provides a class called Machine Learning Crash Course on ML. Our goal is to examine how AI and cyber safety are being advised by MOOCs for the public in general. Systems analysis of research is conducted on academic research on cybersecurity MOOCs. Studies for individual classes are studied, their explanation and design theory, as primary concern is how AI is being taught.

3. Structured Cybersecurity

Assorted organizations have begun to start accumulating and sharing cybersecurity data with other organizations. Different data structures have been proposed for such information in form of XML schemata; e.g., CEE gives computer event data structure and MMDEF gives malware metadata data structure. Also, numerous identifiers and enumerations have been suggested, such as CVE (Popular Vulnerabilities and Exposures) for vulnerabilities, CCE for configurations, CPE for IT properties, and CWE for weaknesses. Please note that all of these works often describe schemes for representing the material identified. One solution is to create the uniform scheme for the exchanging of knowledge that will promote operations. The optimal data structure therefore varies by operation and could be preferred in the future with a different data structure. One-size-fits-all approaches are avoided.

3.1 Structured Cybersecurity in Repository

IODEF offers a way for the details of events between stakeholders to be described and exchanged[22]. It describes a model of data for incident management operations and is a single schema, however, as stated in Section II-C, it offers modular extension capabilities. To best understanding, the business is the first successful structured information sharing tool outside corporate boundaries through computers. Although the number of companies using the tool is not high at the moment, it will make security operations much simpler. However, the data model specified by the IODEF is not rigid, and the user can enter free unstructured text in many fields. The human operators understand these unstructured free texts as well as have a rich source of knowledge; robots can not understand this information. It is not possible to automatically process the information without being organized inside the IODEF records. Additional mechanisms are essential for the automatic collection of information on the incident within the IODEF.

3.2 Repository platform for structured cybersecurity

The IODEF-SCI, an IODEF extension framework to embed standardized knowledge about cybersecurity is introduced in this section. Extension framework is shown in Figure 1.

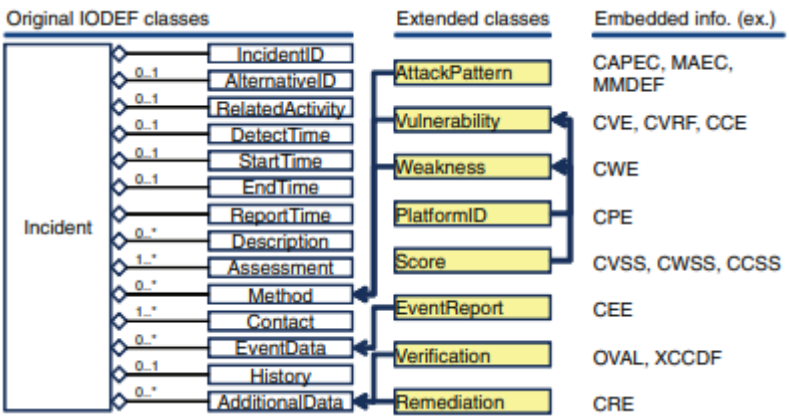

Figure 1: Overview of Repository Cyber Structure Class

IODEF-SCI describes 8 classes, which provide structured knowledge for embedding into an IODEF text.

1. Attack Pattern: This class defines the occurrence or case assault patterns. It is used to supplement method class.
2. Vulnerability: The flaws that were revealed or abused events are listed in this class. . It is used to supplement method class.
3. Scoring: This class defines the security severity ratings. It is meant to supplement and is aligned with the insecurity and weakness classes.
4. Weakness: This class defines the types of vulnerabilities which can be found or used in situations. It is used to supplement method class.
5. Platform: A software framework is defined by this class. It is used to supplement and is combined with the classes Attack Pattern, Vulnerability, Weakness, and Method.
6. Event Report: This class integrates formal monitoring activities. It is used for supplement and associating the Event Data Type.
7. Verification: This class describes safety verification details for treating incidents. It is used to supplement and refer to the event type.
8. Remediation: This class defines details on incident remediation and directions. It is used to supplement to and refer to the event type.

4. Definition of Cybersecurity Structure Class

As an extension of Additional Knowledge Class IODEF with type "xml" the extended classes are introduced. All of the classes have same class structure, as shown in Figure 2,

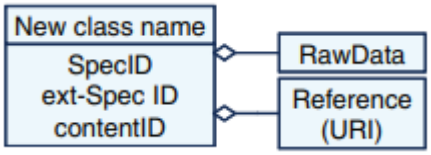

Figure 2: Structure of Repository Class

There are three characteristics for the structure: SpecID, ContentID and ext-SpecID. SpecID is specifier that defines format of standardized data on cybersecurity. The value is chosen from or is "private" from namespaces in organized knowledge table (see Section III-D). For conveying standardized data based on format that is not specified in table, value 'private' is given. It is typically used to transmit data formatted according to private schema of an entity. Ext-SpecID is an attribute utilize only when "private" is value of SpecID attribute. Identifier is told by this attribute of particular standardized cybersecurity information format. Notice that any string can be used here, so that a private schema which is not specified in standardized information table can be supported by IODEF-SCI. ContentID is a standardized knowledge identifier that is intended to bereported. This attribute enables IODEF-SCI to convey organized knowledge identifier instead of conveying data itself. Meaning of this attribute varies slightly according to IODEF-SCI classes, but fundamental definition remains the same. In case of Attack Pattern class, it is an identifier of attack pattern details. Similarly, in case of Platform, this is a platform data identifier, event data, vulnerability data, weakness data, a check item and remediation data, Vulnerability, Weakness, Event Report, Remediation classes, and Verification respectively.

Framework also has 2 components; RawData and Reference. RawData is a complete SpecID/ext-SpecID formatted document specified by specification and its edition. Relationship is a class defined by IODEF. This aspect allows an IODEF document to provide a link to structured information instead of directly embedding it into a RawData element. RawData, Reference and ContentID elements have same specifics with a distinct notation style. Whenever available, it is preferred to RawData or Comparison, since size of data is reduced. While IODEF-SCI classes share same basic structure, to enhance their functionality, some classes have extra elements. In addition to fundamental structure, Vulnerability class can then be automatically connected to platform and scoring data,

where data on platform describes platform where vulnerability occurs, while scoring data gives magnitude of vulnerability. Likewise, there are Platform and Scoring components in Weakness class.

5. Machine Learning

The structured repositories are applied to an artificial network of neural elements that contains a collection of highly interconnected processing elements that transform several entries into the desired output. The transformation results are determined by the elements ' characteristics and weights related to their interconnections. The network can adapt to the desired outputs by changing the connections between the nodes. In figure 3 BPNN with ML is presented.

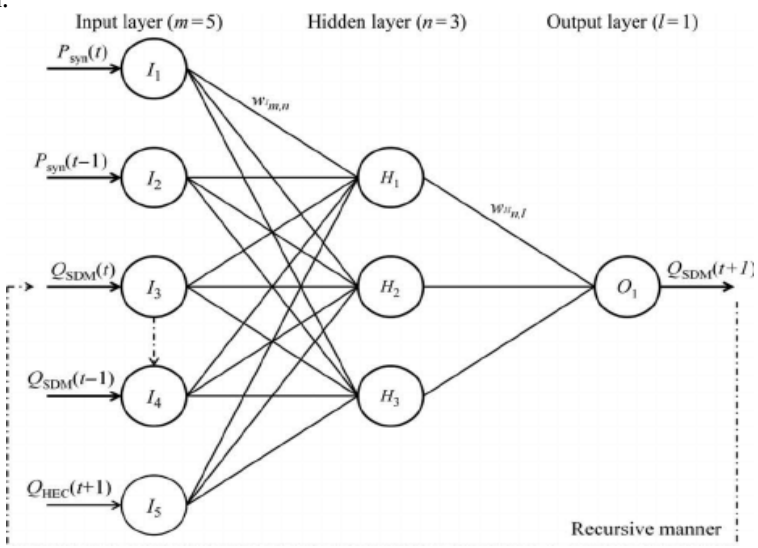

Figure 3: Structure of BPNN in ML

In non-linear solutions to undefined problems, BPNN has the greatest strength. The typical back- up network has an input, output and a hidden layer at least. Number of hidden layers is not theoretical, but typically there are only one or two layers. Several works were done to determine if problems of any complexity are resolved by up to 5 layers. Each layer has a complete connection to the next layer. As indicated above, some variants of the Delta rules are normally used during training and begin with evaluated difference between actual and desired outputs. This error increases connection weights proportionately to mistake times to the global accuracy of the scaling factor. This means that inputs and desired output must all be contained in the same processing element for an individual node.

Complex part of this learning process is that it is system in which input has made most of the wrong output, and how the error is fixed. An inactive node would be unfavorable and no weight change would have to be made. To fix this, training inputs are used on network input layer and desired outputs on output layer are compared. A forward swap is made through network during learning process, and each element's output is calculated layer by layer. Differences between output of final layer and desired output are propagated back to previous layer(s), generally changed by transfer function derivative and weight of connection is normally adjusted according to Delta rule. For previous layer(s), this process continues until input layer is achieved.

Main reasons for adopting BPNN intrusion detection [9] are that the problem of intrusion detection with different characteristics can effectively solve:

(1) There is a large amount of input (training data, including "usual" and "abnormal") /output (various types of attacks, normally typed).

(2) The problem seems to be extremely complex, but a solution is obvious.

(3) Many examples of correct behavior can be created easily.

Thus the appropriate classical BP algorithm is illustrated in Figure 4. It can be used to calculate the intrusion detection task and perform it.

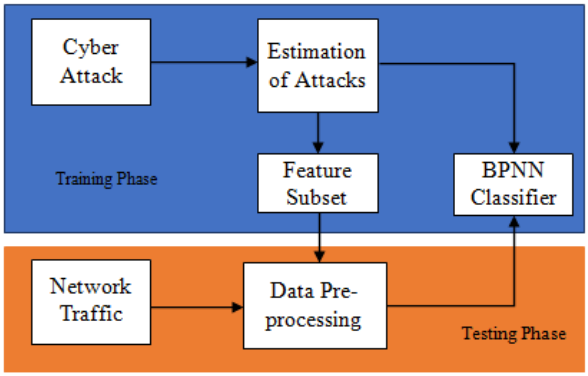

Figure 4: Cyber Attack Estimation using BPNN

(1) At the training stage, labeled network traffic data are transferred to the ICA based feature selection engine with a wide range of preconfigured features (connection time, packet length, SYN / ACK ratio etc.). A reduced feature subset will then be acquired to create BPNN classifier for intrusion detection utilizing selected features with the labeled data set.

(2) In detection stage, network traffic data is sent directly to our BPNN intruder detection classifier after the feature subset has been preprocessed.

Our lightweight model has the greatest benefit of reducing the redundant and irrelevant intrusion detection features using an ANN-based feature selection [10], thus cutting computed costs for intrusion detection.

5.1 Structured Cybersecurity Information Table

IODEF-SCI is supposed to stretchable. It embeds information on organized cybersecurity specified by industry parameters. In a table called the standardized knowledge table, the criteria it may implement are specified. There are the following fields in each entry in the table.

```
<AdditionalData dtype="xml">
 <sci:AttackPattern
  SpecID="http://xml/metadataSharing.xsd">
  <sci:RawData dtype="xml">
   <malwareMetaData
    xmlns="http://xml/metadataSharing.xsd"
    xmlns:xsi=
    "http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation=
    "http://xml/metadataSharing.xsd
    file:metadataSharing.xsd"
    version="1.200000" id="10000">
    <company>N/A</company>
    <author>MMDEF Generation Script</author>

.......omitted.......

   </malwareMetaData>
  </sci:RawData>
 </sci:AttackPattern>
</AdditionalData>
```

1. Namespace: The URI used for the registered specification is the name of the XML namespace.
2. Specification name: A string that includes in human-readable form the spelled out names of the specification.
3. Version: A number that identifies specification version.
4. Reference URI: A list of one or more URIs that can be used to obtain the registered specification. The reported data must be accessible from the URI readily and publicly.
5. Applicable Classes: Only Extended Classes in registry entry must use the registered specification.

Table 1: Structured Cybersecurity Information

Parameters	**Definition**
Name	urn:ietf:params:xml:ns:mile:mmdef:1.2
Version	1.2
Specification	Malware Metadata Exchange Format
Classes	Attack
Reference	http://grouper.ieee.org/groups/ malware/malwg/Schema1.2/

In structured information Table I displays a sample entry. A new entry is added to the table when a new industry standard with new formats is established. The IODEF-SCI can accommodate future requirements by preserving the table and is therefore expandable.

6. Performance Analysis

We set up two standalone devices to evaluate the tool's performance and allow them to use the software to share the IODEF-SCI documents. Specifications of computers are shown in Table 2. Two tests have been carried out with computers.

Table 2: Specification of Parameters

Parameters	**Specification**
Operating System	Windows 8 64-bit
Disk	128 GB SSD
CPU	Intel Core i5 @2.00 GHz
RAM	4.0 B

Next, the validation period was analyzed. Ready-made IODEF, CVE, CPE, CWE, MMDEF, and CCE papers. An IODEF-SCI document created by integrating CPE, CWE, MMDEF, CVE and CCE documents into IODEF document was also prepared. Calculate time five times and computed average value to prevent any unintended variance. These tables show that validating an IODEF-SCI document takes a shorter time than validating each of standardized documents separately. IODEF-SCI text exchange breakdown. The examined mechanism constitutes largest part of activity of information sharing between two organizations.

7. Discussion

This section examines and analyses the proposed scheme and its prototype to prove its usefulness. IODEF is utilized to share user-analyst incident data, between user-side and SOC systems, between SOCs, between SOCs and coordination centers for CSIRT, and between SOCs and SP, including ISPs. Use of IODEF-SCI naturally enables rich material to be shared. For example, the embedding of CVE and CPE identifiers can exchange vulnerability data and vulnerable IT asset data.

Table 3 reveals that extracting the embedded XML was the longest process.

Table 3: Breakdown of Time Consumption

	1st	2nd	3rd	4th	5th	Average
Sending IODEF document	0.18	0.19	0.19	0.19	0.19	0.19
Schema validation	0.09	0.09	0.09	0.1	0.09	0.09
Extracting Embedded XML	1.29	1.21	1.24	1.24	1.25	1.25
Database Registration	0.35	0.32	0.24	0.26	0.28	0.29
Total	1.91	1.81	1.76	1.79	1.81	1.82

To communicate information through computer networks between parties, both sides need to share a similar message format. Many businesses should use and recognize its specifics as to the default IODEF-SCI format. To disseminate the database model, we have already created and submitted it as a request for comments (RFC) to the IETF as a globally agreed specification. RFC defines mandatory-to-implement function to ensure interoperability and allows implementations to parse IODEF with MMDEF version 1.2 without error so that the implementation can be assumed to be compliant with the RFC. The implementation must be able to validate the XML documents obtained that are embedded against their schematics. Notice that in IANA table, recipient will look up the namespace to understand what requirements the embedded XML documents obey. Organized table of information is then transferred to an IANA table, so that experts can manage it. We promote more IODEF-SCI users through this activity.

The above BPNN classification was applied to the data set for the network traffic, which contains both good and bad files. The 10-fold cross-validation has been repeated to ensure that classifier generates data well to unseen information. Table 4 shows results of accuracy, precision, and sensitivity over 10-fold cross-validation after 1000 iterations.

Table 4:Comparison of cyberAttack

Performance Metrics	**Accuracy**	**Precision**	**Sensitivity**
BPNN-IDS for cyberattack detection	0.97	0.96	0.94
BPNN-IDS for shellcode detection	0.93	0.92	0.90
ANN for cyberattack detection	0.92	0.91	0.89
ANN for shellcode detection	0.89	0.86	0.88
Simple IDS for cyberattack detection	0.84	0.82	0.81
Simple IDS for shellcode detection	0.80	0.83	0.81

In table 5 cyber attack instances estimated for developed ML attack detection are presented.

Table 5: Estimation of ML for BPNN in Cyberattack detection

	TruePositive	**false positive**	**false negative**	**TrueNegative**

Actual_class1	4	19	21	56
Actual_class2	25	21	31	23
Actual_class3	3	28	16	53

Furthermore, a very large dataset of candidate network data traffic information content was tested for the performance of the best skilled classification. One key driver of it is that if too many false positives are flaked by a network intrusion detection system, this becomes useless because any true malicious code is drowned off by misidentified benign traffic. To test this, the data was extracted from 500,000 random files in the same format (consisting of log files, text files, office documents, uncompressed or compressed music files, .exe files, and miscellaneous files) as the artificial neural network expected, with this brain data being used by the classifier. The classifier incorrectly identified 10234 samples across this large- scale data.

8. Conclusion

Cyber defense plays an important role in the information technology field. One of today's biggest challenges was securing data. With each New Year that passes, cybercrime continues to diverge along various paths and so does the protection of the data. This paper examined the cybersecurity factors with estimation of attacks and threats in the network. The analysis is based on consideration of ML with the structured information format. Also, ML utilizes BPNN for effective identification of cyberattacks in the structured format data. The analysis expressed that developed mechanism provides improved attack detection mechanism.

References

1. Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: a comprehensive survey. *The Journal of DefenseModeling and Simulation*, 1548512920951275.
2. Vinayakumar, R., Soman, K. P., Poornachandran, P., & Menon, P. (2019). A deep-dive on Machine learning for Cybersecurity use cases. In *Machine Learning for computer and cybersecurity: Principle, algorithms, and practices*. CRC Press.
3. Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., &Airola, A. (2020, July). AI in Cybersecurity Education-A Systematic Literature Review of Studies on Cybersecurity MOOCs. In *2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT)* (pp. 6-10). IEEE.
4. Takahashi, T., & Miyamoto, D. (2016, April). Structured cybersecurity information exchange for streamlining incident response operations. In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium* (pp. 949-954). IEEE.
5. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017, November). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). In *2017 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 253-259). IEEE.
6. Thomas, L. J., Balders, M., Countney, Z., Zhong, C., Yao, J., & Xu, C. (2019, July). Cybersecurity Education: From beginners to advanced players in cybersecurity competitions. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 149-151). IEEE.
7. Shrobe, H., Shrier, D. L., & Pentland, A. (2018). The Trust:: Data Framework as a Solution to the Cybersecurity Challenge.
8. Xia, H., Li, C., & Shi, M. (2019, June). Design of Repositories of GitHub Recommendation System Based on Ternary Closure and HITS Algorithm. In *2019 IEEE/ACIS 18th International Conference on Computer and Information Science (ICIS)* (pp. 1-5). IEEE.
9. Lorchat, J., Pelsser, C., &Fontugne, R. (2014, September). Collaborative repository for cybersecurity data and threat information. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)* (pp. 83-87). IEEE.
10. Zhang, Y., Fan, Y., Hou, S., Ye, Y., Xiao, X., Li, P., ... & Xu, S. (2020, August). Cyber-guided Deep Neural Network for Malicious Repository Detection in GitHub. In *2020 IEEE International Conference on Knowledge Graph (ICKG)* (pp. 458-465). IEEE.
11. Takahashi, T., Panta, B., Kadobayashi, Y., & Nakao, K. (2018). Web of cybersecurity: Linking, locating, and discovering structured cybersecurity information. *International Journal of Communication Systems*, *31*(3), e3470.
12. Devakunchari, R., &Souraba, P. M. (2019). A study of cyber security using machine learning techniques. *International journal of innovative technology and exploring engineering*, *8*(7), 183-186.
13. Jardine, E. (2020). The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity. *Risk Analysis*, *40*(8), 1571-1588.

14. Aldawood, H., & Skinner, G. (2019, January). An academic review of current industrial and commercial cyber security social engineering solutions. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy* (pp. 110-115).
15. Nussbaum, B., & Berg, G. (2020). Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure. *Space infrastructures: From risk to resilience governance*, 91-99.
16. Fowler, D. S., Bryans, J., Cheah, M., Wooderson, P., & Shaikh, S. A. (2019, July). A method for constructing automotive cybersecurity tests, a CAN fuzz testing example. In *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (pp. 1-8). IEEE.
17. DeCusatis, C., Zimmermann, M., & Sager, A. (2018, January). Identity-based network security for commercial blockchain services. In *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 474-477). IEEE.
18. Xu, Y., Wang, G., Yang, J., Ren, J., Zhang, Y., & Zhang, C. (2018). Towards secure network computing services for lightweight clients using blockchain. *Wireless Communications and Mobile Computing*, *2018*.
19. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.
20. Guo, L., Ye, J., & Du, L. (2020). Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks. *IEEE Transactions on Transportation Electrification*.
21. Ashok, A., Hahn, A., &Govindarasu, M. (2014). Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of advanced research*, *5*(4), 481-489.
22. Tehrani, K. (2020). A smart cyber physical multi-source energy system for an electric vehicle prototype. *Journal of Systems Architecture*, *111*, 101804.