Cyber Security Affairs in Empowering Technologies

R .Sri Devi, M. Mohan Kumar

***Abstract**: Digital world connected millions of people through internet for our day today activities, and therefore security, privacy, authentication issues is a key question today. The main objective of this paper is to study various issues in enabling technologies such as Cyber Physical System (CPS), Internet of Things (IoT), Big Data Analytics (BDA) and Artificial Intelligence (AI). IoT is a network of devices which link, interact and transfer data but security and privacy should concern while moving from traditional to modern world. CPS is a combination of data processing, networking and physical activities, through critical infrastructure attacker access computer devices and damages the system. Big data shared high volume, velocity, variety, context and content data to distributed system and key issue is data lost by harm. Artificial Intelligence can perform job as like human brain and solve real world problem but optical network can be easily attacked by hackers. This paper investigate different threats, limitation and future work in the cyber physical system, IoT etc and various methods are discussed from various articles and it is more helpful in doing further research work in this area and cyber security is the most important tool which can be implement to protect the cyberspace from the inside and outside attacker.*

Index Terms: Cyber security, poisoning attack, evasion attack, Intrusion Detection System, tools, deep learning, block chain, algorithm, protocols.

I. INTRODUCTION

Nowadays cyber crime has increased more and more that cause serious losses to government and organization, not only that human are most vulnerable by hackers. Canada is the top most vulnerable country in the world, next India and United Kingdom. Cyber crime is an unlawful access to computer through network for gaining information, damage computer system, hardware, application through any kinds of attacks.

Cyber security is an essential tool for protecting data, sensitive information, and computer devices from the unapproved access. With the modern technologies large amount of data are gathered with low estimate power which lack in security, privacy and interoperability. IoT and CPS are going to play a main role in the cyber space.

Internet of Things (IoT) is centralized network architecture and is more vulnerable to Ransomware attacks and some other attacks because of interconnection with the internet [9]. Mirai virus [7][9] is a malicious program mainly target routers, IP cameras etc, the attacker damaged one million of devices and it is the largest Distributed Denial of Service(DDoS) attack and approachability of some of the websites (Amazon, Twitter, Netflix, The Wall Street Journal etc). In the year 2016, a US domain name server was hacked by (DDoS) attack to gain advantage and perform crime as a service. DDOS is a cyber-attack used to interrupt network traffic to gain resources.

Big data is defined by seven dimensions as 7V's-variety (structure, semi structure and unstructured), volume (peta bytes, Exa bytes, zega bytes, yoga bytes), Velocity(ahead of time- daily, weekly, monthly),Veracity (uncertain content), Value (quality analytics), Visualization(understand data) and Variability (data from different sources)[6] [14].

Artificial Intelligence is a technology plays an crucial role in cyber security to protect from various malicious activities, Advanced Persistent Threats (APTs). AI is used to find vulnerabilities in the network and systems. [19]

The remaining of this paper is arranges as follows: Section II focuses on cyber security in cyber physical system, Section III cyber security in internet of things, Section IV cyber security in Big Data, Section V Artificial intelligence in cyber security and Section VI case study section VII presents discussion and section VIII conclusion and future work.

II. CYBER SECURITY IN CYBER PHYSICAL SYSTEM

Our world is moving ahead robotic surgery in health care, planning for robot soldiers in army etc create various security attacks by hackers and possible vulnerabilities in network traffic etc. Cyber-physical systems are assimilation of cyber and physical component and it is monitored by computer system. Various methods such as quantitative, neural network based risk assessment method have been suggested for identifying vulnerabilities in the CPS. CPS is more vulnerable to cyber-attacks.

Wenbo Wu *et al.* [1] have proposed a quantitative based risk assessment model to identify weakness in the system caused by cyber-attacks. The Pagerank algorithm is used to determine the vulnerabilities in the connectivity of the host and Control algorithm and transmission signal is used to monitor signals in the cyber-physical system. Further they have concentrate on security factors.

Senyu Li *et al.* [2] have found delay speed in the developed neural network and information security is more dangerous due

Revised Manuscript Received on July 08, 2019.

R.Sri Devi, Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-21, Tamilnadu, India. sriha00@gmail.com

Dr. M.Mohankumar, Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-21, Tamilnadu,India. Email ID: mohankumar07@gmail.com

to the changing world of IoT. For indentifying risk factors in cyber-physical system and network most of the researcher suggested Bayesian Network and Wavelet Neural Network (WNN). Here they have proposed a Back Propagation Neural Network (BPNN) method is to examine harm such as information flow control, assets and human factors. The cuckoo search (ICS) algorithm for improving the accuracy and stability of cyber systems and network. The experiments are carryout on MATLAB R2016a. the limitation in this model is to exceed to decrease the running time.

Yang *et al*.[18] examined Intrusion Detection System (IDS) with Deep Learning and Machine learning algorithms for detecting cyber security problems. Recurrent Neural Network (RNN) and Gated Recurrent Unit (GRU) model are used for network security. Wolf *et al*.[12] lack safety and security IoT and CPS, have used safety threat model with coupling technology for both devices.

References	**Tools**	**Descriptions**
[1]	Pagerank algorithm	Websites sorting algorithm by Google search engine
[12]	Coupling technology	To prevent from harmful attacks
[1]	Risk Assessment model	Used to identify risk in medical record
[2]	Cuckoo Search algorithm	Meta-heuristic technique for solve optimization problem
[2]	Mantegna algorithm	Produce random number by process step length
[2]	Bayesian P Neural Network	Suitable for non linear problems
[1]	Control algorithm	Overall system functionalities such as power consumption and controlling robots.
[2]	BPNN –Back Propagation Neural Network	Examine the network intrusion activity in the supervised learning artificial neural network algorithm.
[2]	WNN- Wavelet Neural Network	Used to identified risk assessments in networks.
[18]	RNN- Recurrent Neural Network	Sequence data can be processed
[18]	CNN-Convolutional Neural Networks	Image recognition and speech analysis
[12]	System Synthesis Algorithm	Identified errors and avoid earlier in CPS

III. CYBER SE **SECURITY IN INTERNET OF THINGS**

IoT in going to be a part of our daily activities within a few years and so it is very important to make IoT devices more secure from the hackers. Internet of Things consists of a physical things, virtual assets, and device such as home appliances, various kinds of sensor to monitor smart devices and transmit the data to the cyber world connected through internet.

Shachar Siboni *et al.* [3][4] IoT devices are unsafe to various cyber attacks such as man-in- the-middle attacks, phishing attacks, DOS attacks, sql injection, password sniffing, sensitive data exposure, the major issues is security and privacy is not present while consider IOT. Have first emerged novel security testbed with hardware and software components for testing IoT devices and security is analyzed in network traffic, DOS attack. It contain simulator and stimulators, IoT DUT, security test tools (Metasploit), measurement and analysis tools and penetration test methods are used for the security measurement using machine learning algorithms. In future implementation of security testbed with honeypot environment so researcher can use testbed to test their own IoT appliances.

Andrew Jones *et al.* [4] IoT devices make use of cloud services (Database-as-a-service approach as NoSQL Mongo tool and Storage-as-a-Service)using IPv6 and Wi-Fi for storing large amount of sensor data and therefore user sensitive information are more risk in hands of cyber-attacks. The attacker can easily spread malicious activities, systems malfunction, power failures and security threats while using IoT devices. This paper studied about different kinds of cyber security threats in health care industries.

Shiho Kim *et al.* [5] [25] gave information about implementation of blockchain network in secure and trustable IoT

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

prototype. Blockchain technology is more helpful solution for creating more secure IoT systems [9]. Blockchain is about enabling peer to peer transaction with consensus protocol, immutable distributed ledger, cryptography and smart contract in a decentralized network with record of every transactions and maintained in chronological order . DNSSec is executed for security purpose to intimate attacks in root servers.

Mario Frustaci *et al.*[7] studied Social Internet of Things (SLoT= Social network + IoT) , SLoT connected millions of people through internet to interact and sharing information and interoperability, privacy, security concerns should be emphasized in IoT protocols. Have classified threats into highest, lowest and variable level and identified most vulnerable is perception layer, next transportation and application layer. Have proposed Confidentiality, Integrity, and Availability (CIA) security model in IoT security.

Justin Lipman *et al.*[9][7] studied various issue of code modification and malware attacks on IoT devices , Industrial Control System (ICS) and Cyber Physical System(CPS). This paper extend privacy and security threats of IoT which concentrate mainly on Wireless Sensor Network (WSN) and Radio Frequency Identification (RFID), extended IoT security architecture with three layers. The major two demanding factors in IoT architecture is analyze of the network and logging details.

Ville Sulkamo [26] security issue is the main concern in IoT, has discussed about IoT architecture with Network Mapper, NMAP and NESSUS scanners is used to find threats in the first phase, scanners are installed in kali Linux servers . Raspberry Pi4 computer with big data analytics to collect data and used Pentaho PDI tools. The values are calculated as like as relevant to the SSL protocol. The limitation is security given to IoT appliance is most difficult task.

Walid Saad *et al.* [20] have explained various issues in wireless network such as eavesdropping and illegal gathering of information while transmitting information from one end to other end, suggested graphical Bayesian game approach for Internet of Battlefield Things (IOBT) for maintaining security in the battlefield.

Paul et al. [21] explained problem arising of dark web. The illegal activities can be done in dark web through TOR browser or Virtual Private Network (VPN). Block chain technology can be used for indentified malicious software and this technology is useful related to privacy and security in IoT. Hyperledger Fabric and Ethereum tool is helpful in identifying cyber security problems.

TABLE II. MODELS, PROTOCOLS AND ALGORITHMS

Refe rences	**Tools**	**Descriptions**
[9] [8] [14] [13] [13] [13] [19] [19] [16] [16] [16] [15]	HDFC- Hadoop Distributed File System Google's map reduce HMM- Hidden Markov Model SVM-Support Vector Machine Random Forest (AE) algorithm XG Boost algorithm Optimised XGBoost algorithm WLC - Weighted Lexicon Classifier, VDC- Vector Distance Classifier, RBC- Readability Based Classifier , DWLC- Differential Weights Lexicon Classifier, LBC- Lexicon Based Classifier Honeypots IDS- Intrusion Detection System SNMP- Simple Network Management Protocol SDN- Software Defined Network	Protect sensitive data in BDA Semi supervise method for different kind of attacks machine learning algorithm with accurate and robust method Used for regression and classification problems Machine learning algorithm for improving the Performance and speed Multiple classification algorithm for identify neural messages, provide signal in big data analytics Improve performance and speed Record attacks and intrusions in security aspects for information security Identify malicious activities monitor, configure, control elements in network devices Cluster management

IV. CYBER SECURITY IN BIG DATA ANALYTICS

In olden day's graph, statistical and econometric models concerned for data analytics, but nowadays data files are collected from various sources [14].

Uzma Afzal *et al.* [6] have proposed security analytics model used for threat detection and studied various issues in BDA. [9] HDFC (Hadoop Distributed file System) and Google's MapReduce tool is used to process very large sets of data in the file system but it is insufficient to secure sensitive information.

Teoh *et al.* [8] presented a approach Hidden Markov model (HMM) to identify security attacks and Fuzzy k-Means (FKM) algorithm is adopted.HMM is a network security risk analysis and here this model is used for predict time series data. The future work to implement deep learning for larger amount of data.

Nasser *et al.* [13] have studied about various cyber security threats related to big data and Intrusion Detection System. For the first time have developed hyper heuristic and Support Vector Machine (SVMs) configuration model using

Random Forest(RF), XGBoost (AE) and Optimised XGBoost (OXB) algorithms to find accuracy, complexity of various malwares.

Yan *et al.*[16] have designed next generation (5G) network based data collection with security in big data. Have proposed three set of factors such as tools, nodes, mechanisms and different tools and protocols nearly security purpose.

Chiroma *et al.* [14] recommended a model Parallel Back Propagation Neural Network (PBPNN) with Hadoop tool and identified issues in big data with Artificial Neural Network (ANN).

David *et al.* [19] China is a developed nation in the world and it is moving towards digital commerce. This paper recommended Computational Social Science (CSS), Data Science, DM, and Machine Learning (ML) methods for big data analytics in China for empirical research study. A weighted lexicon classifier (WLC), a vector distance classifier (VDC), a differential weights lexicon classifier (DWLC), a lexicon based classifier (LBC) and a readability based classifier (RBC). Hadoop, MapReduce tools are used for data analytics.

TABLE III. MODELS, PROTOCOLS AND ALGORITHM

References	**Tools**	**Descriptions**
[9] [8] [14] [13] [13] [13] [19] [19] [16] [16] [16] [15]	HDFC- Hadoop Distributed File System Google's map reduce HMM- Hidden Markov Model SVM-Support Vector Machine Random Forest (AE) algorithm XG Boost algorithm Optimised XGBoost algorithm WLC - Weighted Lexicon Classifier, VDC- Vector Distance Classifier, RBC- Readability Based Classifier , DWLC- Differential Weights Lexicon Classifier, LBC- Lexicon Based Classifier Honeypots IDS- Intrusion Detection System SNMP- Simple Network Management Protocol SDN- Software Defined Network	Protect sensitive data in BDA Semi supervise method for different kind of attacks machine learning algorithm with accurate and robust method Used for regression and classification problems Machine learning algorithm for improving the Performance and speed Multiple classification algorithm for identify neural messages, provide signal in big data analytics Improve performance and speed Record attacks and intrusions in security aspects for information security Identify malicious activities monitor, configure, control elements in network devices Cluster management

V. ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Leslie [25] AI technology can be used for network monitoring , status of network, IP infrastructure and cyber threats analysis using Resource Description Framework (RDF).

Leslie *et al.* [25] studied network devices and communication flow around the network including router configuration files, open dataset, protocol etc. with fuzzy and possibilistic logics to found problems and more helpful in protecting secure network.

Luis and emil [25] analyzed machine learning algorithm is used by hacker to create threats such as poisoning attack and evasion attack. Have proposed Reject On Negative Impact (RONI) algorithms to identify this kind of attack. MNIST dataset is used for experimental purpose.

Eric *et al.* [25] used various supervised learning approach to study software vulnerabilities. To collect data in dark web and deep web CYR3CON is used.

Alexander and Igor [25] recommended Neural networks, genetic algorithms and fuzzy logic to found network attacks. Support Vector Machine (SVM) approach using binary classifier. DARPA 1998 dataset is used for experimental work.

Jie Li *et al.*[25] explained various threats are rising in network intrusion detection system used KDD 99 dataset using machine learning algorithm for IDS and considered fuzzy C-means clustering technique used whole information.

TABLE 4. VARIOUS TOOLS IN IOT, BIG DATA , MACHINE LEARNING, NETWORK FORENSIC , AI AND ITS DESCRIPTION.

S. No	**Tools**	**Tools Description**
Cyber Security Tools		
1	TANAGRA data mining tool with Rnd tree classification algorithm [11]	• Detect email spam
2	OpenVas tool with PHP info() function [11]	• Removing threats
Big Data Tools (open source)		
3	Microsoft Cognitive toolkit	

	(CNTK) Horizon Tensar Coffee GLUON Pytorch Mxnet	• Standalone machine learning tool • Open source from python, c#, c++
4	Hidden Markov Model [8]	• Forecasting time series
Machine Learning Tools (open source)		
5	Cybernetics Darker	• Data transfer in secure way • Identify Network complexity
6	Auto weka Spearmint	• Computerized selection tool and hyperparameter optimization in WEKA
7	Auto sklearn Auto Keras Auto ML	• Automated Machine learning tool in python
8	Support vector machine(SVM) [18]	• Supervised Learning Model
Network Forensic Tools (open source)		
9	Paraben device seizure Oxygen phone manager SIM seizure software Celldek tek Cellebrite XRY and XACT	• App analysis • Backup files • Recover deleted files • Mobile forensic tool • Data extraction • GPS navigation tool
10	Paragon Oxygen forensic	• Hard drive Partition • Cutting edge technologies • Investigation software and recover all files.
11	Gitrob	• Command line tool
Cyber Physical System Tools		
12	Back propagation Neural Network (BPNN) [2]	• Dataset classification
13	Artificial Neural Network(ANN) [14]	• Modeling, data collection, dynamic control
Internet of Things Tools		
14	Open Web Application security Project(OWASP) [9][26]	• Penetration Testing Tool • Web application security
15	NMAP Nessus [26]	• Network Scanner • Vulnerability scanner
Block Chain Technology Tools		
16	TX protocol-financial transaction [23]	• Resolve security and privacy issues
17	Hyperledger Fabric tool	• Important for IoT protections
Artificial Intelligence Tools		
18	Security Algorithm-Standard Ontology(SASO) [25]	• Threats, vulnerabilities, controls will be identified
19	Cyber Effects Simulation Ontology (CESO) [25]	• Imitate the effects of cyber-attacks
20	Reject On Negative Impact (RONI) [25]	• Alleviate the influence of data poisoning attack
21	Open source databases i)Common Vulnerability Scoring System (CVSS) ii) NVD,EDB,ZDI, DW [25]	• Identified vulnerabilities in information technology
22	Genetic algorithm [25]	• Used in artificial intelligence to solve the problem
23	Network Intrusion Detection System (NIDS) [25]	• Software and hardware tools • Watch the performance of network traffic
24	Mamdani fuzzy model	• Defuzzification progress

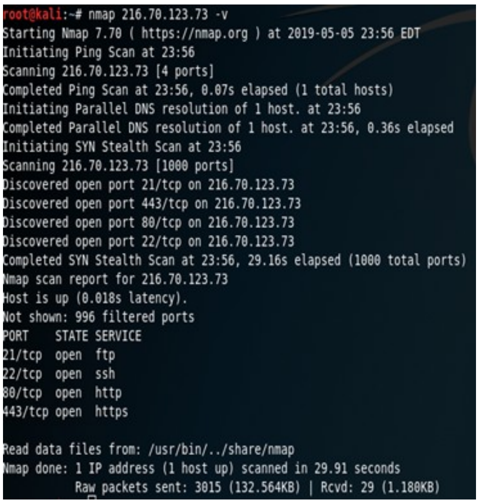
VI. CASE STUDY

We studies some network scanning tools from the above tables to identify the vulnerabilities in the network based on penetration testing methodology including Network Mapper, Nikto and OWASP to get an overview of IP address, host, find servers , gather information about ports and security solution is also given.

The results are given below

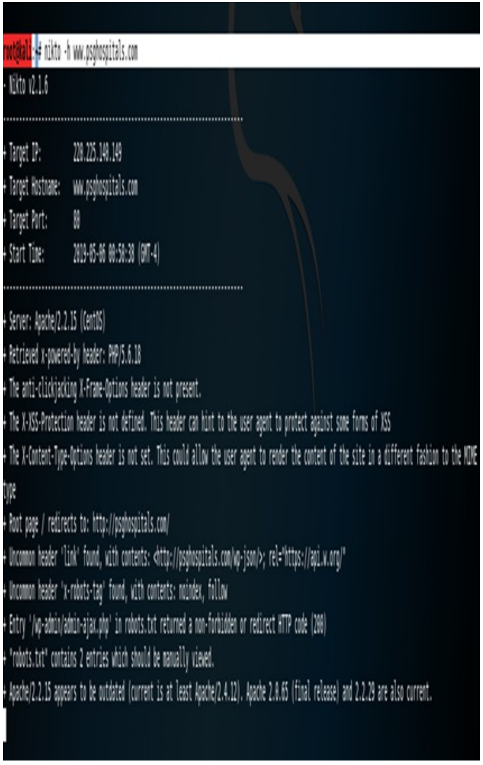
Nmap - Network mapper tool was used for vulnerability scanning and network discovery.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication



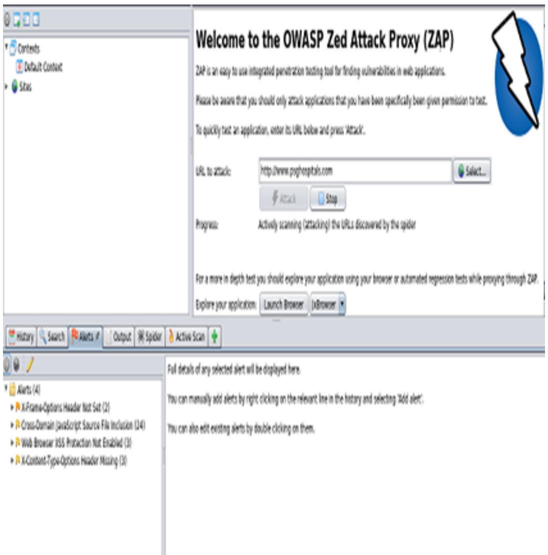
```
root@kali:~# nmap 216.70.123.73 -v
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-05 23:56 EDT
Initiating Ping Scan at 23:56
Scanning 216.70.123.73 [4 ports]
Completed Ping Scan at 23:56, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:56
Completed Parallel DNS resolution of 1 host. at 23:56, 0.36s elapsed
Initiating SYN Stealth Scan at 23:56
Scanning 216.70.123.73 [1000 ports]
Discovered open port 21/tcp on 216.70.123.73
Discovered open port 443/tcp on 216.70.123.73
Discovered open port 80/tcp on 216.70.123.73
Discovered open port 22/tcp on 216.70.123.73
Completed SYN Stealth Scan at 23:56, 29.16s elapsed (1000 total ports)
Nmap scan report for 216.70.123.73
Host is up (0.018s latency).
Not shown: 996 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 29.91 seconds
           Raw packets sent: 3015 (132.564KB) | Rcvd: 29 (1.180KB)
```

- Nikto Web Scanner is used to scan your web site and server immediately for known
  mis-configurations and security vulnerabilities.



```
root@kali:~# nikto -h www.psghospitals.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          220.225.140.149
+ Target Hostname:    www.psghospitals.com
+ Target Port:        80
+ Start Time:         2019-05-06 00:50:38 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.15 (CentOS)
+ Retrieved x-powered-by header: PHP/5.6.18
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
type
+ Root page / redirects to: http://psghospitals.com/
+ Uncommon header 'link' found, with contents: <http://psghospitals.com/wp-json/>; rel="https://api.w.org/"
+ Uncommon header 'x-robots-tag' found, with contents: noindex, follow
+ Entry '/wp-admin/admin-ajax.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.2.15 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
```

- Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is a penetration testers and web application security scanner.



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.psghospitals.com

Progress: Actively scanning (attacking) the URLs discovered by the spider

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

Explore your application:

Alerts (4)
- X-Frame-Options Header Not Set (2)
- Cross-Domain JavaScript Source File Inclusion (24)
- Web Browser XSS Protection Not Enabled (3)
- X-Content-Type-Options Header Missing (3)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

You can also edit existing alerts by double clicking on them.

.

VII. DISCUSSION

From the previous section on Cyber Security in Cyber-Physical System (CPS) (section 2), Cyber Security in Internet of Things (IoT) (section 3), Cyber Security in Big Data Analytics (BDA) (section 4), Artificial Intelligence in Cyber Security (section 5) it is clear that there are various threats and vulnerabilities are happening now a day in the network infrastructure through email, web application and as well from physical environment. However, there is an inadequacy of security and privacy issues in the above technologies. Most of the CPS structure is not designed for security reason and lack in user's privacy. Many techniques are used to sort out the problems and provide solutions. But each and every method has its own merits and demerits. So there emerges the need of fruitful new methodology to prevent the issues

VIII. CONCLUSION

In the present scenario due to rapid development of modern technologies in cyber world we are unsafe in hands of hacker with security and privacy issues. This paper studied various cyber security threats and vulnerabilities in CPS, IoT, BDA an AI. Table 1 describes various open source tool collected from various articles, workshop and conference. Most of field however health care's industries, e-commerce, infrastructure, is vulnerable to malware attack, economic losses, sensitive information, is gathered by the attacker for financial benefits. From the studied it is cleared that flaws in network is the main reason for security. Most of the researcher worked with HADOOP and Spark is useful for sizable dataset, but generating variety of data creates issues in big data analytics. Block chain technology, Public key cryptography, machine learning algorithm etc is the most recommended tool for cyber security in health, energy and industrial sector. To protect the world from cyber crimes cyber security tools must be implemented in all the enabling technologies. The aim of this paper is to do further research in this area. In addition the paper be used as a preliminary stage for researchers eager in this technologies.

REFERENCES

1. Wu, W., Kang, R., & Li, Z. (2015, December). Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities. In Industrial Engineering and Engineering Management (IEEM), 2015 IEEE International Conference on (pp. 1618-1622). IEEE.
2. Li, S., Bi, F., Chen, W., Miao, X., Liu, J., & Tang, C. (2018). An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking. IEEE Access, 6, 10311-10319.
3. Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S.,& Elovici, Y. (2018). Security Testbed for Internet-of-Things Devices. IEEE Transactions on Reliability.
4. Abouzakhar, N. S., Jones, A., & Angelopoulou, O. (2017, June). Internet of Things Security: A Review of Risks and Threats to Healthcare Sector. In Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017 IEEE International Conference on (pp. 373-378). IEEE.
5. Singh, M., Singh, A., & Kim, S. (2018, February). Blockchain: A game changer for securing IoT data. In Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on (pp. 51-55). IEEE.
6. Mahmood, T., & Afzal, U. (2013, December). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. In Information assurance (ncia), 2013 2nd national conference on (pp. 129-134). IEEE.
7. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet of Things Journal, 5(4), 2483-2495.
8. Teoh, T. T., Nguwi, Y. Y., Elovici, Y., Cheung, N. M., & Ng, W. L. (2017, July). Analyst intuition based Hidden Markov Model on high speed, temporal cyber security big data. In 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD) (pp. 2080-2083). IEEE.
9. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of Threats to The Internet of Things. IEEE Communications Surveys & Tutorials.
10. Hodgson, R. (2019). Solving the security challenges of IoT with public key cryptography. Network Security, 2019(1), 17-19.
11. Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (pp. 307-311). IEEE.
12. Wolf, M., & Serpanos, D. (2018). Safety and security in cyber-physical systems and internet-of-things systems. Proceedings of the IEEE, 106(1), 9-20.
13. Sabar, N. R., Yi, X., & Song, A. (2018). A bi-objective hyper-heuristic support vector machines for big data cyber-security. IEEE Access, 6, 10421-10431.
14. Chiroma, H., Abdullahi, U. A., AlArood, A. A., Gabralla, L. A., Rana, N., Shuib, L., & Herawan, T. (2018). Progress on Artificial Neural Networks for Big Data Analytics: A Survey. IEEE Access.
15. Wu, J., Dong, M., Ota, K., Li, J., & Guan, Z. (2018). Big data analysis-based secure cluster management for optimized control plane in software-defined networks. IEEE Transactions on Network and Service Management, 15(1), 27-38.
16. Lin, H., Yan, Z., Chen, Y., & Zhang, L. (2018). A survey on network security-related data collection technologies. IEEE Access, 6, 18345-18365.
17. Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, 3(4), 208-218.
18. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., & Wang, C. (2018). Machine learning and deep learning methods for
19. cybersecurity. IEEE Access, 6, 35365-35381.
20. Phang, D. C., Wang, K., Wang, Q., Kauffman, R. J., & Naldi, M. (2019). How to derive causal insights for digital commerce in china? a research commentary on computational social science methods. Electronic Commerce Research and Applications, 100837.
21. Abuzainab, N., & Saad, W. (2019). A graphical Bayesian game for secure sensor activation in internet of battlefield things. Ad Hoc Networks, 85, 103-109.
22. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks.
23. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174.
24. Makhdoom, I., Abolhasan, M., & Ni, W. (2018, August). Blockchain for IoT: The Challenges and aWay Forward. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications-Volume 2: SECRYPT. INSTICC.
25. Wang, E. K., Ye, Y., Xu, X., Yiu, S. M., Hui, L. C. K., & Chow, K. P. (2010, December). Security issues and challenges for cyber physical system. In 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE.
26. Sikos, L. F. (2018). AI in Cybersecurity (Vol. 151). Springer.
27. Ville Silkamo (2018) IoT from cyber security perspective case study JYVSECTEC. (pp 1-98)
28. Saqib Ali et al (2018) Cyber Security for Cyber Physical Systems, Studies in computational intelligence, volume 768

AUTHORS PROFILE

R.Sri Devi, Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-21, Tamilnadu, India. sriha00@gmail.com

Dr. M.Mohankumar, Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-21, Tamilnadu, India. Email ID: mohankumar07@gmail.com