FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

Effective Cyber Security Using IoT to Prevent E-Threats and Hacking During Covid-19

Dr. Santosh Kumar[1], Dr. Rajeev Yadav[2], Dr. Priyanka Kaushik[3], S B G Tilak Babu[4], Dr. Rajesh Kumar Dubey[5] and Dr. Muthukumar Subramanian[6]

[1]*Asso. Prof., Lucknow Public College of Professional Studies, Lucknow, Uttar Pradesh, India, sanb2lpcps@gmail.com*
[2]*Professor in CSE, Arya Institute of Engineering and Technology, Jaipur, Rajasthan, India, yadavrajeev6@gmail.com*
[3]*Asso. Prof. in CSE, Poornima Institute of Engineering and Technology, Jaipur, Rajasthan India, Kaushik.priyanka17@gmail.com*
[4]*Dept. of ECE, Aditya Engineering College, Surampalem, thilaksayila@gmail.com*
[5]*Asso. Prof., Department of Electrical Engineering, Central University of Haryana Mahendergarh-123031 India, rajesh.dubey@cuh.ac.in*
[6]*Dept. of CSE, SRM Institute of Science & Technology, Trichy Campus, Tamilnadu, India - 621105, drsm.iiit@gmail.com*

***Correspondence:** -- S B G Tilak Babu; Email: thilaksayila@gmail.com

ABSTRACT- This research work is conducted to make the analysis of digital technology is one of the most admired and effective technologies that has been applied in the global context for faster data management. Starting from business management to connectivity, everywhere the application of IoT and digital technology is undeniable. Besides the advancement of the data management, cyber security is also important to prevent the data stealing or accessing from the unauthorized data. In this context the IoT security technology focusing on the safeguarding the IoT devices connected with internet. Different technologies are taken under the consideration for developing the IoT based cyber security such as Device authentication, Secure on boarding, data encryption and creation of the bootstrap server. All of these technologies are effective to its ground for protecting the digital data. In order to prevent cyber threats and hacking activities like SQL injection, Phishing, and DoS, this research paper has proposed a newer technique of the encryption process by using the python codes and also shown the difference between typical conventional system and proposed system for understanding both the system in a better way.

General Terms: Cryptography, Cryptanalysis, Pattern recognition, Data Security, Hacking.

Keywords: Interdisciplinary, Cyber security, Theory of computation, Internet of Things (IoT), E-threat.

ARTICLE INFORMATION

Author(s): Dr. Santosh Kumar, Dr. Rajeev Yadav, Dr. Priyanka Kaushik, S B G Tilak Babu, Dr. Rajesh Kumar Dubey and Dr. Muthukumar Subramanian

Special Issue Editor: Dr. Sandeep Kautish
Received: 21/03/2022; **Accepted**: 20/04/2022; **Published**: 15/05/2022;
e-ISSN: 2347-470X;
Paper Id: 0222SI-IJEER-2022-02;
Citation: 10.37391/IJEER.100210
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100210.html

This article belongs to the Special Issue on **Novel Architectures and Methods in Industrial IoT and Wireless Sensor Networks for Sustainable Computing**

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

1.1 Background

Advanced technology has widely changed today's world. By utilizing, IoT based digital technology, various complex tasks can be done faster without any error. Moreover, the digital-based technology also offers to operate the tasks like business operation, progress monitoring, and financial transaction through online processes. Moreover, data management also gets quite easier and more efficient as well after the rapid implementation of IoT technology. These kinds of wide diversified facilities effectively help the spread the usage of the IoT technology in the market faster [1].

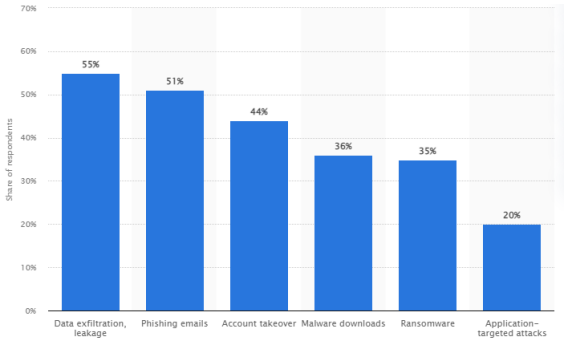


Figure 1: Cyberattacks during a pandemic

During pandemics, the incidents of cyber-attacks have been increased regardless of the location and industry. More specifically, most of the cyber-attacks that happened during this time are related to data exfiltration leakage and phishing the sensitive emails. This helps in analyzing the fact that the need of identifying the different IoT tools and methods used are needed to be analyzed.

1.2 Purpose

The main purpose of this research work is to demonstrate the ways the different cyber security methods and tools used in the time of pandemics to protect users from hackers or cyber

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

attackers.

2. LITERATURE REVIEW

2.1 The role of cyber security to prevent e-threats and hacking

E-threats are a kind of serious threat to mankind that causes due to unethical malpractices over the internet. The e-threats involve the unfair means of the intention like frauding, stealing data and developing security breaches for fulfilling the purpose of the data theft. In order to prevent this, the concept of cyber security has been introduced [2]. It is working as one of the major effective drivers of business success in the competitive business market. The main function of cyber security is that provide constant support and security by creating an encrypted environment. IoT based encrypted environment is usually developed with numerous loops in which hacking software fails to freely works. In such a process, the monetary transaction can be done flawlessly [3].

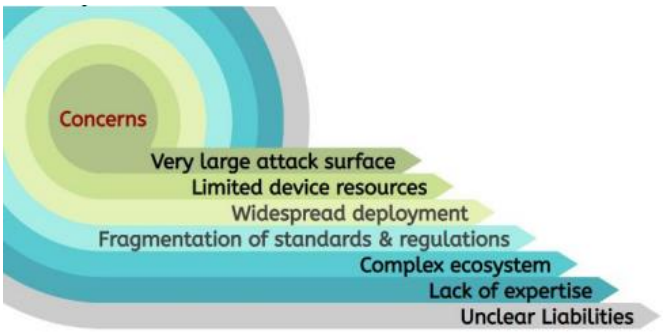


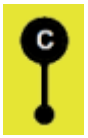
Figure 2: Security Consideration for IoT

Although the main obstacles of developing and using IoT is already outlines, others are visualized in the diagram. In the functional area of the IoT, the integration and updating the infrastructure, heterogeneity and inherent complexity is count as a security challenge.

2.2 Understanding of the problem domain

An effective application of a cyber-security system within a business helps an organization achieve its desired position in the global market. However, cybersecurity issues are rapidly increasing in organizations affecting their market reputation and customer satisfaction largely. The domain of cyber security includes various challenges that include - breaching of cyber security, unauthorized access to data, and several others [4]. Third-party unlawful intervention causing misuse of the network is one of the biggest challenges faced by the modern-day along with other challenges that include mobile malware as well. Artificial intelligence as one of the most rapidly growing technologies has the potential to deal with cybersecurity issues. The growing popularity of IoT technology and AI has paved the way for minimizing the negative impact of cyber security and its challenges significantly.

Table 1: Sixth of the most critical IoT attack

Scenario	Level of Impact	Threats	Scenario	Impact level	Threats
Linking network in between actuators and controllers		**Sensitive data leakage**	**Administrative system of IoT**		**Attacks on privacy, DDoS, Malware**
Modification of the values read by the sensors		Leaking of the sensitive data due to the attacks on privacy	Injection of the additional commands in the system console		Network outage, weak password, DDos
Sabotaging or modifying ACUATORS normal setting		Counterfeit the security software by malicious devices	IoT botnet can be sued to stop DDoS action		Exploit kits, DDoS

Social engineering, data breaches and phishing is increasing exponentially in the recent years. In this context critical and high risk factor based threats are marked with H& C resp. In case the threats increased too high to critical, then both letters are noted. Based on the Okiru and Mirai malware this paper has developed the security system by using machine learning.

The rapid increase of cyber-attacks and multiplication of devices occurring in today's technology-driven world accelerated the necessity of adopting artificial intelligence to address these cybersecurity issues. Cybersecurity threats can broadly be divided into 7 types including Malware, Emotet, Service Denial, Man in the middle, Phishing, Password Attacks, and SQL injection [5]. A detailed discussion of the above-mentioned cyber threats might help in developing an understanding of the problems that this domain faces.

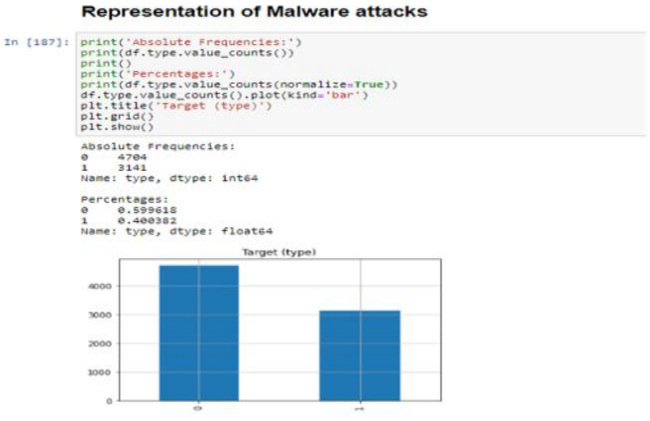


Figure 3: Representation of various malware attacks

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

2.3 Malware

Malware is a kind of malicious software that includes ransomware, viruses, spyware, and others that are activated by cybercriminals to block access to major network components. This kind of cyber threat also causes the automated installation of harmful software and obtains data covertly by transmitting them from the system hard drive [6]. Malware threats to a system can also disrupt individual parts of that system making them completely inactive. To mitigate such threats, effective infrastructure is required. The circulation of this type of malicious software got common, especially during Covid-19. Based on a survey it has been found that during the time of global pandemic situation, hackers have been spread some fake news related to Covid-19 along with links where they injected the malicious virus [7]. Now, when a major number of social media users have shared the same circular message without knowing anything in-depth, the malware effectively captures more devices. Thus in the following way, it has been impacted the digital transmission of the data.

2.3.1 Emotes

Emotet malware is regarded as a Trojan initially developed as a banking malware for sneaking onto the computers of others to steal private information. However, the later versions included the addition of malware delivery and spamming devices in the system along with other banking Trojan. The use of worm-like capabilities by this software has helped in spreading to other connected computers ensuring the distribution of the malware [7]. The extensive spread of this malware needs the intervention of advanced technology to stop spreading.

2.3.2 Service denial

DoS or denial of service is a kind of cyber-attack that swamps a computer or a network making it able to respond to requests. A flood attack is often used by cyber attackers to hamper the handshake process and to execute DoS [8]. Distributed DoS works similarly to DoS, however, the origination of the attack is done from a computer network. Through DDoS or distributed DoS, millions of systems can get affected by the control of the attackers or hackers.

2.4 Existing methods and associated advantages and disadvantages

2.4.1 Threat detection and incident response framework

Threat detection is an essential aspect to prevent cyber-attacks. On that note, the steps that are needed to be taken are identified through such a response framework. The major advantage of this type of system is that it can help in reducing resource and time wastage. However, the different schools of thought have expressed that having no insider threat program can be disadvantageous when it is not incorporated into such a system [9].

2.4.2 IPS (INTRUSION PREVENTION SYSTEM)

IPS is identified to be another existing tool used by the cyber security teams to prevent cyber attackers from obtaining personal or sensitive information. The major benefit of using this tool is that malicious activities can be identified in real-time and it has included the next-generation firewall in the system. On the other hand, this technology is criticized for lacking speed when an organization does not have high bandwidth capacity. Besides, it has also been identified that this type of technology requires high network capacity and a company lacking such an aspect can face this type of issue [10]. Therefore, loss of performance due to incapable operations is a major disadvantage of using this tool.

2.5 Phishing

This unique attack is executed by cyber attackers through fake communication such as e-mail to trick the receiver into opening that mail and making them carry out information such as debit or credit card details to steal money from the respective bank account [11].

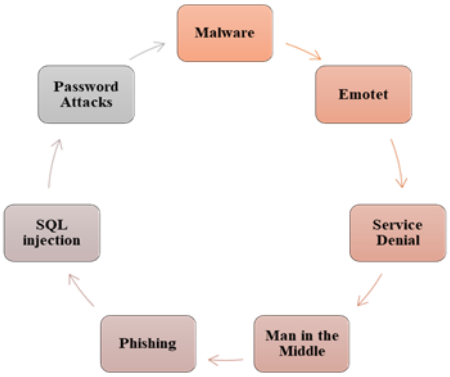


Figure 4: Different types of problems

2.6 SQL Injection

Structured query language or SQL injection is a type of cyber-attack that is caused by the insertion of malicious code into a SQL using server. Getting infected by the code the server starts releasing information regarding the network. This is one of the easiest ways of attacking a network using SQL.

2.7 Password attacks

Access to people's passwords allows hackers to a plethora of information regarding the victim and their confidential accounts [12]. This attacking strategy is highly dependent on human interaction or manipulation of people, compelling them to break standard security practices which were common during Covid-19.

3. RESEARCH METHODOLOGY

Research methodology is one of the significant parts of this research in which the researcher has been highlighted all the evidence of the research topic for satisfying the research objectives. It is quite evident that during the Covid-19 pandemic most customers have started to gain digital experience due to the national and international lockdowns imposed by the government of the UK and other countries. The restriction on the mobility suddenly increase the usage of the IoT for functioning digital transaction and other works. It

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

is to be noted that with the increment of the usage of the cybersecurity, the chances of data hacking also gets higher. In this context, the protection of customers' information is crucial since the hacking of customers' data can cause trouble and financial losses for the companies as well as the individuals. Hence, with the immense efforts made by the researcher in the research, this study has demonstrated a range of research evidence, which depicted that the use of IoT and other technologies could reduce the threats of cyber hacking during the covid-19 pandemic.

Cross domain. An advanced data driven approaches to develop the security refers to the umbrella term Cybersecurity data science.

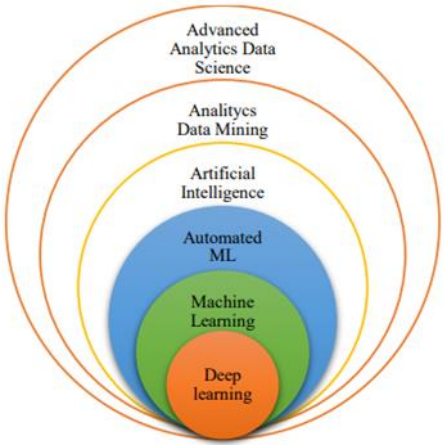


Figure 5: Knowledge discovery of Paradigm

Synergetic is usually applied for the different tactics to determining the significant relationship between the diverse research fields to finding out the optimal solution. In the selection of sample method, the researcher has chosen one of the appropriate sampling methods for gathering the responses of the people belonging to the UK market. There are two types of sampling methods that are "The probability sampling method and the Non-probability sampling method". Therefore, the researcher has used the probability sampling method in which people from the UK industry has chosen randomly for obtaining the responses so that he could complete the research work within time. Moreover, the main reason for ignoring the non-probability sampling by the researcher is it could not be beneficial for the researcher in obtaining the research evidence. Therefore, the help of probability sampling method has helped the researcher in obtaining the responses about the necessities of IoT during the Covid-19 pandemic for reducing the risk and threats of cybercrime. Lastly, it is illustrating that the experimental sampling method could also be beneficial for the researcher in obtaining reliable information from different experiments in the research.

From the above discussions that the experimental method of data collection has played a significant role for the researcher in completing the research work with much ease and accuracy. On the basis of the research study it has been found that there are usually 7 types of cyber security threats may appear, such as Emotet, Malware, and Man in the middle, Denial of services, SQL injection, Phishing and Password attack. In order to protect the data from such kind of cyber-attack, the precautionary measures like network security, cloud security and IoT security can be implement. In this context, this research paper has followed *IDPS method*.

4. RESULT, ANALYSIS AND INTERPRETATION

This research paper has considered mixed methods such as primary quantitative or survey and secondary qualitative methods to develop a better understanding based on the role of cyber security using IoT for preventing hacking and e-threats during Covid-19. To develop the quantitative information, the survey strategy has been chosen effective and on that note, 31 people or respondents have been selected from whom the required information is taken.

Design of the security system

Context: IoT cybersecurity
Data: Light labelled version, IoT-23 public dataset
Infrastructure: OS Windows server, 2019, 6 CPU, 32GB RAM
Platform, libraries and language: Python 3.8
Classifiers: Decision tree (DT), random forest (RF), Logistic Regression (LR)
Algorithm: Bayesian Algorithms, Regression algorithms, Instance based algorithm

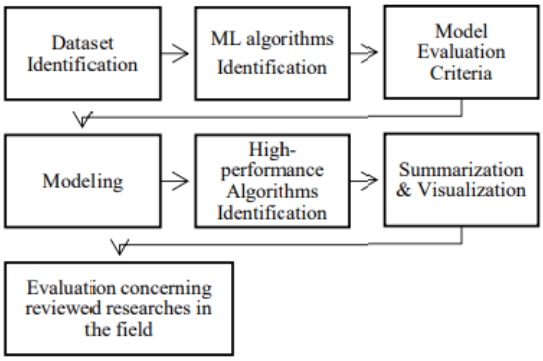


Figure 6: Process of the system development

The above *figure* has demonstrated the process of developing the security based software. For checking the malicious scenario, a sample of specific malware are taken and analyzed by using Raspberry Pi and its several protocols. Multiclass dataset has been considered for adequate evaluation metrics.

		NB		SVM		LR		DT		RF	
		S04	S16	S04	S16	S04	S16	S04	S16	S04	S16
Accuracy		0.58	0.58	0.72	0.74	0.76	0.75	1.00	1.00	1.00	1.00
Precision	W	0.75	0.76	0.68	0.70	0.74	0.73	1.00	1.00	1.00	1.00
Recall	W	0.58	0.58	0.72	0.74	0.76	0.75	1.00	1.00	1.00	1.00
F1 Score	W	**0.51**	**0.48**	**0.68**	**0.70**	**0.73**	**0.72**	**1.00**	**1.00**	**1.00**	**1.00**
Runtime	sec	2.63	8.91	0.71	1.24	0.72	1.23	0.86	1.10	48.04	66.42
CPU	%	100	100	222.3	425.9	219.5	430.5	99.9	100	100	100
Memory	%	4.43	5.68	5.31	5.33	7.25	8.72	4.26	11.81	11.14	18.79

Figure 7: Classifier evaluation metrics

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

The Naïve Bayes classifier (NB) has shown the worst performance among the other models Support vector machine (SVM) and Logistic Regression (LR).

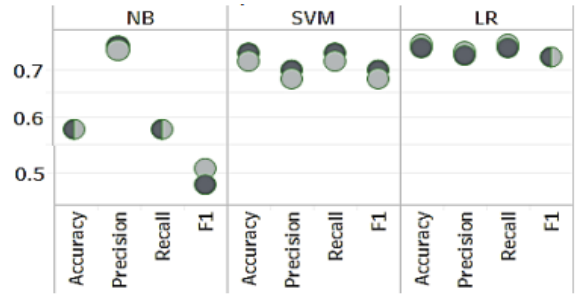


Figure 8: Metrics variation

The above figure has demonstrated the result by comparing the metrics variation in between NB, SVM and LR.

5. DISCUSSION AND FINDINGS

5.1 Threat recovery using python coding

In the present context, socially engineered attacks are the most common. Social engineering attacks are not limited to phishing, emails, and others, which work through the manipulation of human psychology. In order to protect this,

Import Python Libraries

```
In [159]: import pandas as pd
          import numpy as np
          import seaborn as sns
          import matplotlib.pyplot as plt
          from sklearn.model_selection import train_test_split
          from sklearn.naive_bayes import GaussianNB
          from sklearn.model_selection import train_test_split,cross_val_score
          from sklearn.metrics import classification_report
          from sklearn.metrics import confusion_matrix
```

(Source: Created by the researcher)

Figure 9: Importing of Python libraries

In order to protect the system from the threats, python coding based antivirus and cybersecurity can be build up. In this context, at the initial stage, python libraries are need to import.

Drop NaN Columns

```
In [162]: df.drop('avg_local_pkt_rate',axis='columns', inplace=True)
In [163]: df.drop('avg_remote_pkt_rate',axis='columns', inplace=True)
In [164]: df.drop('duracion',axis='columns', inplace=True)
In [165]: df.head()
Out[165]:
```

	name	tcp_packets	dist_port_tcp	external_ips	vulume_bytes	udp_packets	tcp_urg_packet	source_app_packets	remote_app_packets	source_app_bytes
0	AntiVirus	36	6	3	3911	0	0	39	33	5100
1	AntiVirus	117	0	9	23514	0	0	128	107	26248
2	AntiVirus	196	0	6	24151	0	0	205	214	163887
3	AntiVirus	6	0	1	889	0	0	7	6	819
4	AntiVirus	6	0	1	882	0	0	7	6	819

Figure 10: Dropping of NaN columns

Nan value in Python programming is considered as a floating-point value that is subject to conversion into other data types of float. In the analysis of data, the NAN value is regarded as unnecessary that needs to be removed to ensure proper analysis of data. Here the above-mentioned figure is reflecting the various NaN value of Antivirus that include *external_ips*, *vulume_bytes*, *source app_app packets*, and others.

Object to Integer Conversion

```
In [168]: df['type']=df['type'].astype('category').cat.codes
In [169]: df.head()
Out[169]:
```

	name	tcp_packets	dist_port_tcp	external_ips	vulume_bytes	udp_packets	tcp_urg_packet	source_app_packets	remote_app_packets	source_app_bytes
0	AntiVirus	36	6	3	3911	0	0	39	33	5100
1	AntiVirus	117	0	9	23514	0	0	128	107	26248
2	AntiVirus	196	0	6	24151	0	0	205	214	163887
3	AntiVirus	6	0	1	889	0	0	7	6	819
4	AntiVirus	6	0	1	882	0	0	7	6	819

Figure 11: Object to the integer conversion

Object to integer conversion in Pandas programming converts data into a numeric type. Through the function of *Pamdas. to_numeric ()* this conversion into an integer is executed. In the above-mentioned figure, numeric objects have been converted into integers. Such kind of numeric data is not readable by other devices that effectively provides an efficient protection by establishing IDBS.

Updating devices and their firmware regularly is another mitigating strategy. Backup of all kinds of sensitivities and non-sensitivities data is also essential that usually performed by AI system under the encrypted environment. Thus in the following way, e-threats and hacking like activities can be mitigated.

5.2 Integration and implementation of AI with IoT

To implicate artificial intelligence in different organizations having the concept regarding human intelligence, simulation has been evaluated. To protect sensitive data from theft and to avoid malware, especially during the higher usage of IoT, like the Covid-19 pandemic, these types of intelligence are applicable. Some critical steps of implementing artificial intelligence are,

(*i*) Being familiar with the AI is the primary step

(*ii*) Identification of the problems is the next step

(*iii*)The values that are being prioritized to deal with the scenario is the most concerning step that needs to be understood while integrating AI

(*iv*)Development of a pilot project to bring up the expert opinion and to set the plan is the ultimate step to implicating AI

(*v*) Formation of the task force to deal with the integrated data is important in this scenario.

(*vi*)Choosing the right artificial intelligence systems that can work better than human intelligence with the machine learning process to simplify the algorithms is the ultimate state that needs to be maintained as well.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2| Pages 111-116 | e-ISSN: 2347-470X

6. CONCLUSION

Cyber-attacks are on the rise with more sophisticated technology arriving at the scene. Ransomware has been the most recent which nearly disrupted the entire data processing services in the digital world. The business has become vulnerable to these kinds of attacks due to some structural deficiency in the industry as well as unethical business practices. The deficiency of robust security systems and infrastructure comes as a secondary threat. As per the above discussion, it has been noticed that during the time of Covid-19, while the usage and demand of IoT is high due to physical mobility restrictions, that time try to take a higher level of the chance of data hacking. Considering this fact, IoT based cyber security has been considered in this study for protecting digital devices. Encryption based approaches are also has been considered in this study for meeting the purpose of it. In terms of explaining the future direction of cyber security the increased rate of attacks is seen. The demand taking place in cyber security is going to be increased quickly in the coming future due to its successfully stopping e-threats. To develop this technique to some extent, the python coding can be executed by aligning with the AI technology. Such a method may assist to discover the internet pressure in a smarter way and could be able to implement the hacking tools.

REFERENCES

[1] Ibrahim, H., Karabatak, S. and Abdullahi, A.A., 2020, June. A study on cybersecurity challenges in e-learning and database management system. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

[2] Zhao, J., Liu, X., Yan, Q., Li, B., Shao, M., Peng, H. and Sun, L., 2021. Automatically predicting cyber-attack preference with attributed heterogeneous attention networks and transductive learning. Computers& security, 102, p.102152.

[3] Ding, A.Y., De Jesus, G.L. and Janssen, M., 2019, September. Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure. In Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing (pp. 49-55).

[4] Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. Future Internet, 12(9), p.157.

[5] Bertino, E., and Islam, N., (2017). Botnets and internet of things security. Computer, (2), pp. 76-79.

[6] Laszka, A., Zhao, M., and Grossklags, J. 2016. Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms. Computer Security – ESORICS 2016 Lecture Notes in Computer Science, pp. 161-178.

[7] Abdullah, T.A., Ali, W., Malebary, S. and Ahmed, A.A., 2019. A review of cyber security challenges attacks and solutions for the Internet of Things based smart home. Int. J. Comput. Sci. Netw. Secur, 19(9), p.139.

[8] Singla, M.K., Gupta, J., Nijhawan, P., Ganguli, S. and Rajest, S.S., 2020. Development of an Efficient, Cheap, and Flexible IoT-Based Wind Turbine Emulator. In Business Intelligence for Enterprise Internet of Things (pp. 225-231). Springer, Cham.

[9] Matheu-García, S.N., Hernández-Ramos, J.L., Skarmeta, A.F. and Baldini, G., 2019. Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, pp.64-83.

[10] Sriram, S., Vinayakumar, R., Alazab, M. and Soman, K.P., 2020, July. Network flow based IoT botnet attack detection using deep learning. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 189-194). IEEE.

[11] Hossain, M., Islam, S.R., Ali, F., Kwak, K.S. and Hasan, R., 2018. An internet of things-based health prescription assistant and its security system design. Future generation computer systems, 82, pp.422-439.

[12] Ibrahim, H., Karabatak, S. and Abdullahi, A.A., 2020, June. A study on cybersecurity challenges in e-learning and database management system. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

[13] Chandrajeet Yadav, Vikash Yadav and Jasvant Kumar (2021), Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-based Encryption in Cloud Environment. IJEER 9(3), 48-56. DOI: 10.37391/IJEER.090305.