FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 105-110 | e-ISSN: 2347-470X

Intelligent Solutions for Manipulating Purchasing Decisions of Customers Using Internet of Things during Covid-19 Pandemic

Dr Avinash Rajkumar[1], Pankhuri Agarwal[2], Dr Mohit Rastogi[3], Dr Vipin Jain[4], Dr Chanchal Chawla[5] and Dr Manoj Agarwal[6]

[1,2,3]Asst.Prof., Teerthanker Mahaveer Institute of Mgmt. & Technology, Mahaveer University, Moradabad, Uttar Pradesh, India
[4]Prof., Teerthanker Mahaveer Institute of Mgmt. & Technology, Mahaveer University, Moradabad, Uttar Pradesh, India
[5,6]Asso.Prof., Teerthanker Mahaveer Institute of Mgmt. & Technology, Mahaveer University, Moradabad, Uttar Pradesh, India

*__Correspondence:__ Dr Vipin Jain; Email: vipin555@rediffmail.com

ABSTRACT- It is a well-known fact that consumers may gain significant benefits from the effective use of IoT in pandemic and post-pandemic settings. Security vulnerabilities can be seen in the ever-increasing Internet of Things (IoT) ecosystem from cloud to edge, which is crucial to note in this particular circumstance. Most merchants, even luxury stores, have failed to implement robust IoT cyber security procedures. Therefore, the researchers sought to put forth secondary research methodologies to bring forward efficient scrutiny regarding this particular issue to properly comprehend the influence of IoT in various devices, including a smartwatch, power displaying metre, brilliant weight showing gadgets and many more. The secondary research approach allowed the researchers to collect a large quantity of data quickly, acquiring a wide range of possible solutions for security and privacy issues in Consumer IoT (CIoT) devices. Secondary research also will enable scholars to compare and contrast several papers' philosophies and research findings to get a quick conclusion. To gather information, the researchers used publications and the internet efficiently. In this situation, it helped to save a significant amount of time.
Findings suggested that vulnerabilities occur in smart IoT gadgets, including the intelligent power consumption metre and brilliant weight displaying widget, due to their low-standard and conventional security system. Thus, this paper has suggested possible solutions to protect IoT devices against phishing and theft attacks.

General Terms: Technology Acceptance Framework, CENTRON Smart Metre.

Keywords: Artificial intelligence, Consumer Internet of Things (CIoT), Secondary research analysis, Smart gadgets, Security.

ARTICLE INFORMATION

Author(s): Dr Avinash Rajkumar, Pankhuri Agarwal, Dr Mohit Rastogi, Dr Vipin Jain, Dr Chanchal Chawla and Dr Manoj Agarwal

Special Issue Editor: Dr. Sandeep Kautish
Received: 29-03-2022; **Accepted**: 20/04/2022; **Published**: 15/05/2022;
e-ISSN: 2347-470X;
Paper Id: 0222SI-IJEER-2022-03;
Citation: 10.37391/IJEER.100209
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100209.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

"The Internet of Things ", popularly known as IoT, refers to the "physical objects"; this particular element is assimilated with different software, sensors, and tools to connect and diversify data with other connected devices. Different retail sectors are employing it significantly to maintain their supply chain efficiently during the global covid-19 pandemics [1]. The digital economy put forward many hurdles and opportunities during the covid-19 pandemic, including IoT's heavy employment in business scenarios. The outbreak of the novel coronavirus has systematically massacred the entire structure of functioning of the world [2]. In this particular scenario, it is important to mention that the basic structural pattern of the disease was pulmonary. It is also important to mention that serious cardiovascular influence was witnessed during this treatment. Numerous governments formulated applications that were put forward in this particular scenario, such as "covid-19 alert "by Canada, "Stop Corona" by Australia, "Immuno" by Itali and many other applications. Different organizations have also employed various official tracking applications and symptoms tracker applications.

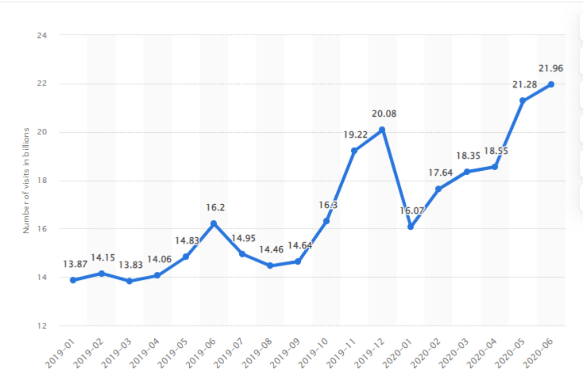
To assist the patients and other people effectively, different marketing and consumer goods organizations put forward different machine learning approaches in this scenario so that further details can be fetched to put forward efficient service to the consumers [3]. An example must be put forward in this scenario that symptoms trackers were invented in the kings' College London to manoeuvre the symptoms of the diseases effectively. Despite the benevolent initiatives of the university and healthcare system, the data of the public becomes vulnerable due to this [4].

"The Internet of Things ", popularly known as IoT, refers to the "physical objects"; this particular element is assimilated with different software, sensors, and tools to connect and diversify data with other connected devices. Different retail sectors are employing it significantly to maintain their supply chain efficiently during the global covid-19 pandemics. The digital economy put forward many hurdles and opportunities during the covid-19 pandemic, including IoT's heavy employment in business scenarios. The outbreak of the novel coronavirus has systematically massacred the entire structure of functioning of the world [2]. In this particular scenario, it is important to mention that the basic structural pattern of the disease was pulmonary. It is also important to mention that serious cardiovascular influence was witnessed during this treatment. Numerous governments formulated applications that were put forward in this particular scenario, such as “covid-19 alert “by Canada, “Stop Corona” by Australia, “Immuno” by Itali and many other applications. Different organizations have also employed various official tracking applications and symptoms tracker applications.

To assist the patients and other people effectively, different marketing and consumer goods organizations put forward different machine learning approaches in this scenario so that further details can be fetched to put forward efficient service to the consumers [3]. An example must be put forward in this scenario that symptoms trackers were invented in the kings’ College London to manoeuvre the symptoms of the diseases effectively. Despite the benevolent initiatives of the university and healthcare system, the data of the public becomes vulnerable due to this [4].

In this particular scenario, it is essential to mention that because of massive data manipulation, be it in the healthcare sector or the consumer goods sector, the serious cyberattack is wreaking havoc during the pandemic [5]. Therefore, it is essential to implement security measures so that the hurdles associated with the security issues can be mitigated effectively in the healthcare sector and in the marketing sector to predict consumer behavior effectively. In this scenario, it is essential to mention that the "Conditional privacy-preserving technique” can be put forward to effectively ensure the safety of the data vailed during the pandemic in the health sector and the business sector [6]. This particular technique is manoeuvred in a systematic pattern that ensures the privacy of data of the users and consumers while retrieving the information of the server data effectively. It means that it systematically assist in protecting the data put forward by the users and consumers while shopping or enlisting themselves in the symptoms trackers. At the same time, it effective assist to identify the unauthorized tracking in the device of the users installed with this tool.

Additionally, an interesting angle can be put forward in this scenario that due to the increase of the pandemic, people are becoming more and more reliant on the internet while shopping and doing other things. An enormous increase in online shopping can be effectively witnessed in this particular scenario. However, the data the portals access during shopping make the consumers vulnerable in the face of different cyber-attacks. Many people, especially the aged ones, still fear transacting through this method. Therefore, the security of the data must be maintained while doing an online activity while maneuvering the consumer’s decision at the time of purchasing, even though the pandemic compelled the people to put forward online transactions. Back to the normal situation can effectively affect online shopping, which would systematically affect consumer decisions. Therefore, the data protection aspect must be manoeuvred in a rigid pattern so that people can feel protected while shopping and doing online activities. This paper will effectively try to analyses the influence of AI in influencing the purchasing decision while ensuring data safety.



(Source: [7])

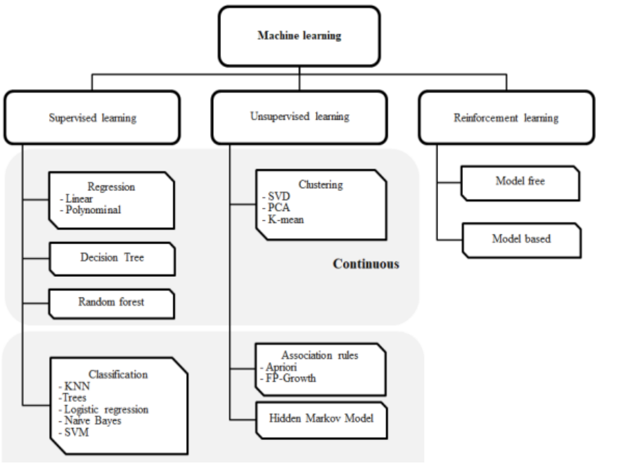
Figure 1: The Influence of Pandemic n Retail E-Commerce

2. LITERATURE REVIEW

When discussing this particular situation, it is necessary to point out that, as the covid-19 pandemic continues to spread, many individuals are turning to online transactions to fulfil their needs and requirements. It is possible to notice an increase in the number of occurrences of data breaching. Some folks are adamant about not using this media because of the unapproved hazard. The organizations putting up their proposals must avoid unauthorized tracking while dissecting the behavioral pattern of the consumers while keeping the security of the transaction for more people to use a comparable platform to satisfy their essential requirements. In this situation, a graph can be used to illustrate the point. As a result of the pandemic, shopping websites and media outlets have seen unprecedented increases in traffic volume never previously seen. This is a clear indication of the popularity of internet purchasing. However, it also increased the likelihood of a data breach occurring. As a result, a security procedure must be proposed after analyzing the consumer's behavior pattern.

In the opinion of some researchers, it is necessary to mention that artificial intelligence-enabled machine learning tools effectively assist in maximising the potency of a computer-based programme while also ensuring data safety and data protection effectively through the use of the lucid method on sample pieces of information and previous experiences. As a result, in this scenario, a framework with qualities, parameters, and determinants was proposed to perform computer operations properly and maximise the framework’s potency by adding the trained pieces of information from previous experiences. This framework is proposed to effectively foresee or preach the absorbed knowledge or news that has been derived from the data. In this circumstance, it is necessary to point out that AI-enabled machine learning is nearly identical to core statistics since the critical crux of the ML framework is linked with the core framework of statistics. Many researchers have offered exciting insights into this particular scenario. Here are a few examples.

They asserted that statistics is concerned with the interpretation of data manipulation, whereas machine learning is concerned with the fundamental characteristics of algorithms [8]. It efficiently assists in bringing forward an efficient insight into the possibility of customer behaviour while making a purchasing decision through AI-enabled machine learning. It also correctly secures the data collected from consumers. When making a purchasing decision, machine learning combines efficient algorithms capable of analysing the "pattern of cluster customer behaviour" seen. The fact that this same technique also takes into account independent determinants such as "term identification, decision-tree, impartial server, SVM manipulation" that effectively assist in predicting consumer behaviour while making a purchasing decision while ensuring the data protection accuracy in this particular domain is essential to note in this specific scenario [9].



(Source: [10])

Fig 2. The Instances of Machine Learning

Other researchers argue that the "Technology Acceptance Framework," popularly known as "TAM", is a framework that effectively assists in systematically analysing the consumers' behavioural patterns while making a purchasing decision while ensuring safety. It systematically put forward comprehension and insight to reach end-users on how the consumers adapted to the technology. In this particular scenario, it is essential to mention that this framework is designed with the efficient assistance of the "Technology Acceptance Framework". It systematically assists to display a lucid understanding to comprehend consumer behaviour, communication, impressions and other things. In this particular scenario, it is essential to mention that external determinants play a significant role in this scenario, such as experience, preconceived belief, data safety, comprehension, etc.

It is essential to mention in this particular scenario that to put forward motivation of the customer for the expensive products, the marketing department of the organisation must assess those external determinants to incorporate encouragement to the consumers so that they can witness the influence of value in that particular product of service while ensuring the data security aspect of the domain. At the same time, it is essential to mention that this specific technology can be very efficient in administering the conformity of the users.

At the same time, this technology can effectively assess the behavioural pattern and the intention to employ the technology. This particular technology effectively comments on the effect of the external determinants vehemently. From three perspectives, it has emphasised "belief, interest, attitude and many other elements". They are 1. The idea of the influence of the tools 2. The concept of the convenience of the technology 3. The perception of security while employing this technology. Additionally, in this scenario, it is essential to mention that this framework tends to align itself with the idea of technology perception to formulate behaviour that can be dissected as the employment of the tool. Most of the consumer goods organisations in the UK tend to employ this technique to interpret the purchasing decision making of the consumer while assuring data safety.

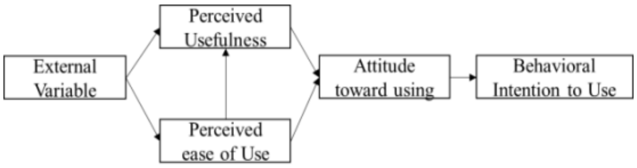


Fig 3. Technology Acceptance Framework

On the other hand, different researchers commented in this particular scenario that AISAS effectively comments on the buying pattern of the consumers while tapping into the data from the internet. It also systematically considers the previous buying pattern of the consumers. However, it does not employ unauthorised tracking of the consumers' devices. It means that safety issues are manoeuvred efficiently with the effective employment of AI while putting forward sort after products as per the desirability of the consumers. The working scenario of this framework works in a fascinating pattern. It begins when a consumer notices a product, and the intention is stimulated to fetch more details regarding a similar product or service. This framework follows five steps known as "attention", "interest", "search", "action", and "share". Amazon started to opt for this framework during pandemics to influence consumers' decisions while maintaining data safety effectively.

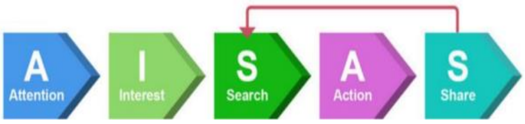


Fig 4. The Steps of the AISAS Framework

3. METHODOLOGY

To understand the data privacy and security concerns in CIoT, the researchers have tried to put forward secondary research methods to put on efficient scrutiny regarding this particular topic. The secondary research method effectively enabled the researchers to gather a significant amount of data in a short period to get a broad perspective of the scenario. The secondary research also enables the researchers the ideologies and research results of different articles to pit against each other to reach an imminent conclusion. The researchers have effectively employed journals and internet sources to fetch information. It effectively assisted in saving an enormous time in this particular scenario. Moreover, previously conducted research provided the researchers with a broad outline of how they should proceed to reach a legitimate conclusion. The researchers have employed peer-reviewed journals in this particular scenario, which helps them considerably in their research. At the same time, peer-reviewed journals enable them to maintain the authenticity of the information during the course. Additionally, the researchers have tried to employ articles from the past decade to maintain the regency aspect of the research properly.

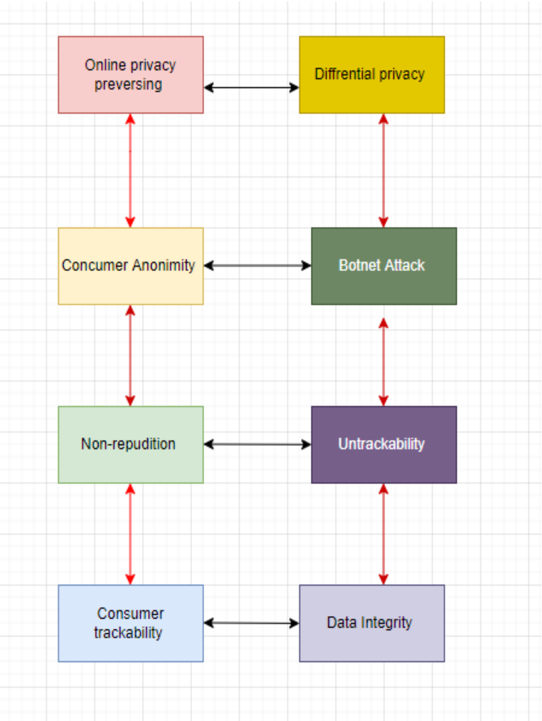


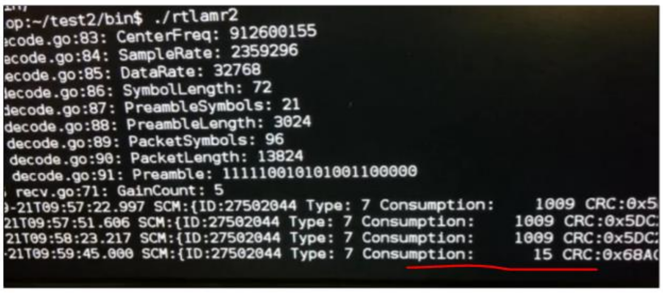
Fig 5. Flowchart of the security breaches

Research Questions:

1. What are the advantages of employing IoT in consumer device controlling applications?
2. What are the risks and opportunities associated with the privacy and security facilities of CIoT?
3. What are the advanced solutions of IoT to protect consumer devices?

4. ANALYSIS AND INTERPRETATION

A new CIoT device is CENTRON Smart Metre which is used in houses and industries to collect real-time electricity data usage and utilities. The vulnerability and attack in this are an attacker can access the entire hardware system of this metre and manipulate the circuit to change readings [12]. Reports have observed the vulnerabilities and attacks on this smart metre, resulting in energy theft and economic loss. When the users do not observe the power readings carefully, phishing may occur. Researchers observed that different power readings were generated with the same metre ID. *Fig. 6* shows the same metre ID; however, the power reading is different.



```
op:~/test2/bin$ ./rtlamr2
ecode.go:83: CenterFreq: 912600155
ecode.go:84: SampleRate: 2359296
ecode.go:85: DataRate: 32768
lecode.go:86: SymbolLength: 72
decode.go:87: PreambleSymbols: 21
decode.go:88: PreambleLength: 3024
decode.go:89: PacketSymbols: 96
 decode.go:90: PacketLength: 13824
 decode.go:91: Preamble: 111110010101001100000
 recv.go:71: GainCount: 5
-21T09:57:22.997 SCM:{ID:27502044 Type: 7 Consumption:     1009 CRC:0x5
21T09:57:51.606 SCM:{ID:27502044 Type: 7 Consumption:     1009 CRC:0x5DC
21T09:58:23.217 SCM:{ID:27502044 Type: 7 Consumption:     1009 CRC:0x5DC
-21T09:59:45.000 SCM:{ID:27502044 Type: 7 Consumption:      15 CRC:0x68A
```

Fig. 6. Same metre ID with different readings of the power

The possible reason for this attack is that the "EEPROM chip" present inside the smart metre is not highly secure against the attacks. Therefore, a tamper-resistant development can mitigate the issues by utilising "Physically Unclonable Functions" or PUF. It is a great alternative that introduces digital fingerprints. The digital fingerprint does not allow any unauthorised access [14].

Certain vulnerabilities are likely to occur which include the software failure where an attacker inputs wrong passwords and still receives an entry into the IoT devices. Studies suggest that Charger point of Electric vehicles (EV) "ChargePoint Inc" has an authentication phase through "Branch if equal" or BEQ. The attackers target this authentication phase and get the entry into the device with a wrong password [15]. It was identified that IoT device developers are not focusing on the security system and developing new features to attract their consumers which is resulting in security breaches.

An intelligent solution for mitigating these vulnerabilities is to replace strcpy() with strncpy(), which has been shown to strengthen IoT security in EV charging techniques. Another validation or authentication can be integrated using "Uploadsm" during the file modification. Researchers also found that in the consumer EV, different types of OS command injection vulnerabilities are arising. The possible solution for its mitigation is "Validation of String" using Uploadsm. Other vulnerabilities and challenges are the "buffer overflow" of the stack and log files. Possible solutions for them is to integrate "Length Specifier" in sscanf() [16].

Another CIoT device is Smart Aria Air, a human weight displaying machine connected to the mobile application Fitbit. After measuring the weight, the information is transferred to the mobile application, where the BMI is displayed to the user and a quick trend for better health. The user's information is transferred to the Fitbit server using wireless technology, and the fitness guidelines and advice are provided accordingly. In that wireless data transfer, attackers use Wireshark to collect information transferred from that intelligent device. Moreover, the attackers can access the log file and "Pre-shared Key", which ultimately allows the attacker to gain access to the users' home network. After the entrance, the attacker can access other devices associated with the home network [17].

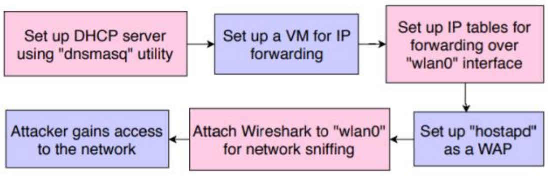

Set up DHCP server using "dnsmasq" utility
Set up a VM for IP forwarding
Set up IP tables for forwarding over "wlan0" interface
Set up "hostapd" as a WAP
Attach Wireshark to "wlan0" for network sniffing
Attacker gains access to the network

Fig. 7. Flow diagram of attack on Smart Fitbit Aria

It has been identified that IoT device developers are not focusing on data encryption at every single point of wireless data transfer. Studies suggest that Fitbit Aria does not have an encrypted communication system between the device and server, allowing the attackers to access the log and key files through a communication channel. Therefore, advanced encryption techniques rather than conventional techniques will help encrypt the essential data. Block chain technology can be a possible solution for this IoT device [18]. Apart from this, a "Virtual Private Network" or VPN can be used to tunnel the communication into an encrypted system. The VPN can be defined as an 'encrypted tunnel' for transferring and receiving data; however, the internet needs to be turned off after using a VPN. Otherwise, the attackers can access the home Wi-Fi [19].

On the other hand, many researchers expressed their concern regarding the security issues in this domain. It is not a hidden fact that retailers can efficiently reap huge fruits with the efficient employment of IoT in pandemic and post-pandemic scenarios. However, in this scenario, it is essential to mention that security vulnerabilities can be witnessed vehemently in the ever-increasing IoT ecosystem from cloud to edge. Most retailers, even luxury retailers, fail to adopt strict IoT cyber security measures associated with it. The pandemic has made this particular scenario more problematic as the employment of IoT tools are employed at a significant rate. If one delves deep into these specific issues, it can be identified that there are core seven challenges associated with IoT security. They are -

- Weak password safeguard
- Omission of regular patches
- Weak update mechanism
- Lack of security in the interface
- Poor data protection
- Inefficient IoT device administration
- The gap in the IoT efficiency

5. DISCUSSION AND FINDINGS

There is no doubt that the consumer's spending would maximize due to the core incorporation of AI that effectively dissects a massive chunk of data manipulation that sort out the information in such a pattern that assists the organization in recognizing the target audience. Machine learning nowadays can affect the behavioral pattern of the consumers effectively while analyzing the requirements of the consumers. The AI-enabled machine learning tool effectively assists in putting forward trend analysis so that organizations can incorporate consumer-focused marketing tactics that would effectively enable the organization to score conversations of the potential target audience.

In this scenario, it is essential to mention that with the efficient assistance of AI, one can effectively comprehend what consumers are looking at and how many times they visit a particular website. Therefore, the organization must incorporate "predicative personalization" to create an even better consumer experience. In this specific domain, it is essential to identify that with the incorporation of covid-19 pandemic, most people cannot go to an offline store. Therefore, the traffic online is ever-increasing. Organizations must look at this particular situation as an opportunity to maximize the consumer's online experience so that the consumer's purchasing decision can be manipulated for the greater good. Effective implementation of AI can systematically promote the concept of "Virtual shopping", where some products are sent to consumers' places after identifying their behavioral patterns on the internet through machine learning [20].

However, it can be also be seen that during various covid-19 cyber-attacks have been put forward, and data security of the consumers had been compromised in this process. In the year 2021, *Mozi* was utilized by hackers. It is considered a sub-variant of *Mirai* which wreaked havoc in 2017 that almost obliterated wen services put forward by Amazon, Netflix, Twitter and mother organizations. *Mozi* is considered one of the most active botnets in recent times. The infrastructure of this botnet is maneuvered mainly from *China*'s land. It is also important to mention in this particular domain that *Japan* and *USA* have been bombarded with the efficiency of this botnet. Therefore, all retailers must employ different optional mechanisms such as *password complexity, expiration, profile lock-out techniques*, *OTP methods* and many other techniques. These techniques enable the retailers to improve and store the provided credential while employing a particular IoT device. Additionally, *biometric substantiation, multi-factor verification, Two-factor confirmation* must be used by the organizations to make sure that no unrecognized access can be maneuvered in the connected IoT devices and servers [21].

6. CONCLUSION

This paper has effectively tried to shed light on the influence of advanced security and privacy settings in CIoT devices. The report does not shy away from the fact that the pandemic has opened an enormous opportunity for organizations to promote online and virtual shopping, and efficient use of AI can systematically assist in identifying consumer behavior efficiently. It enables the organization to launch specific marketing strategies to convert them into their value chain. However, a curious case has occurred due to the by-product of this particular scenario. An unprecedented growth can be witnessed due to the maximization of the traffic. Therefore, the organization needs to look after the security issues while providing an efficient consumer experience. Researchers have systematically employed secondary research techniques to gather more substantial information regarding the topic to comprehend some intelligent security solutions for IoT devices. This secondary research has tried to uphold the possible answers for strengthening the security system of CIoT devices without any field experiment. Thus, the suggestions from this study can be experimented with by other researchers to validate them.

REFERENCES

[1] Dankan Gowda V, K. R. Swetha, Namitha A R, Manu Y M, Rashmi G R and Veera Sivakumar Chinamuttevi (2022), IOT Based Smart Health Care System to Monitor Covid-19 Patients. IJEER 10(1), 36-40. DOI: 10.37391/IJEER.100105.

[2] Statista.com, (2021). Coronavirus impacts retail e-commerce website traffic worldwide as of June 2020 by average monthly visits. Available at: https://www.statista.com/statistics/1112595/covid-19-impact-retail-e-commerce-site-traffic-global/

[3] Chaudhary, K., Alam, M., Al-Rakhami, M.S. and Gumaei, A., 2021. Machine learning-based mathematical modelling for prediction of social media consumer behavior using big data analytics. Journal of Big Data, 8(1), pp.1-20.

[4] Y. Y. Zheng, Y. T. Ma, J. Y. Zhang, and X. Xie, “COVID-19 and the cardiovascular system,” Nat. Rev. Cardiol., vol. 17, no.5, pp. 259–260, Mar. 2020.

[5] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, “Digital technology and COVID-19,” Nat. Med., vol.26, no. 4, pp. 459–461, Mar. 2020.

[6] Alladi T, Chamola V, Sikdar B, Choo KK. Consumer IoT: Security vulnerability case studiesand solutions. IEEE Consumer Electronics Magazine. 2020 Feb 3; 9(2):17-25.

[7] Harvard College. Surveys, app. to track COVID-19. [Online]. Available: https://www.hsph.harvard.edu/coronavirus/covid-19-response-public-health-in-action/surveys-apps-to-track-covid-19/, Accessed on: Dec. 27, 2020.

[8] Eian, I.C., Yong, L.K., Li, M.Y.X., Qi, Y.H. and Fatima, Z., 2020. Cyber-attacks in the era of covid-19 and possible solution domains.

[9] Alladi, T., Chamola, V., Sikdar, B. and Choo, K.K.R., 2020. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), pp.17-25.

[10] M. A. Ferran, L. Maglaras, and A. Derhab, “Authentication and authorisation for mobile IoT devices using features: Recent advances and future trends,” Secure. Commun. Netw, vol. 2019, May 2019

[11] Iqbal M, Riadi I. Analysis of security virtual private network (VPN) using openVPN. International Journal of Cyber-Security and Digital Forensics. 2019 Jan 1; 8(1):58-65.

[12] K. Sugiyama and T. Andree, TheDentsu Way: 9 Lessons for Innovation in Marketing from the World's Leading Advertising Agency, McGraw-Hill, 2018.

[13] Harsha, “What is machine learning? Machine learning for beginners,” Big Data Analytics, March, Edureka, 2018.

[14] M. A. Ghazanfar, S. A. Alahmari, Y. F. Aldhafiri et al., “Using machine learning classifiers to predict stock exchange index,” International Journal of Machine Learning and Computing, vol. 7, no. 2, pp. 24-29, 2017.

[15] Loi, F., Sivanathan, A., Gharakheili, H.H., Radford, A. and Sivaraman, V., 2017, November. Systematically evaluating security and privacy for consumer IoT devices. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (pp. 1-6).

[16] Hood KM. Validity and reliability of body composition techniques in healthy adults (Doctoral dissertation, San Francisco State University).

[17] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI) 2017 Apr 18 (pp. 173-178). IEEE.

[18] Wurm J, Hoang K, Arias O, Sadeghi AR, Jin Y. Security analysis on consumer and industrial IoT devices. In2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC) 2016 Jan 25 (pp. 519-524). IEEE.

[19] E. Alpaydin, Introduction to Machine Learning: MIT Press, 2015.

[20] Rauniar, R., Rawski, G., Yang, J. and Johnson, B., 2014. Technology acceptance model (TAM) and social media usage: an empirical study on Facebook. Journal of Enterprise Information Management.

[21] Maes, R., & Verbauwhede, I.M. (2010). Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. Towards Hardware-Intrinsic Security.