Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7765910

SECURITY CONCERNS USING 6G IN THE IOT: BLOCKCHAIN AND MACHINE LEARNING APPROACHES AS A RESCUE

[1]Vidushi, [2]Dr. Manish Bhardwaj, [3]Shweta Singh, [4]Vikas Choudhary,[5]Vinay Kumar
[1,3]Department of Computer Application, KIET Group of Institutions Delhi-NCR Ghaziabad,
[2]Department of Computer Science and Information Technology, KIET Group of Institutions Delhi-NCR Ghaziabad
[4]Department of Computer Science & Engineering-AIML, ABES Engineering College, Ghaziabad
[5]Department of Computer Science and Information Technology, KIET Group of Institutions Delhi-NCR Ghaziabad

ABSTRACT
Internet of Things (IoT) technology is an innovative emerging computing paradigm that provides colossal intelligence to objects interconnected in a huge network. This technology's explosive growth and involvement in the day to day activity, enhances the internet usage gigantically. Size along with the complexity, it is continuously exploding with involvement of more devices universally. Recent trends show that it is becoming an unavoidable technology on society. However, massive information transmission presents severe security challenges that attract scientific community attention. Moreover, in order to tackle security issues and challenges, this paper aim to present an overview of IoT devices, related security concern, and possible solutions using latest advance Machine Learning (ML) and Blockchain technology. This paper highlights current IoT security related research challenges and also discusses avenues for a solution using theoretical holistic blockchain approach. In addition, this document provides an experimental analysis of machine learning relevant approaches as a suitable security solution for IoT devices. Finally, directions for future research in machine learning and blockchain as a rescue for security in IoT is discussed.
Keywords: IoT, Security, Learning paradigms, Blockchain technology, Intrusion Detection System.

1. Introduction

1.1. Background

It has been noted during the last ten years that the Internet of Things (IoT) is a strong contender for modern civilization and a quickly developing technology across a variety of applications. This technology connects billions of heterogeneous devices (includes both physical plus virtual) through wireless media (Internet) and makes them smart. These devices are smart in reference of computing, monitoring, and processing various real-time complex scenarios. This fusion generates voluminous data that might come with momentous security challenges. Admittedly, security-related research should be considered as most dominant aspect for technology advancement. Privacy breach is an unpleasant event for society that becomes a barrier for technologies. IoT model elaborates a huge network of devices which are interconnected through advance capabilities to accomplish various tasks [1]. All IoT devices

in a network are connected directly using the Internet. This increases the possibility of intrusion for IoT devices connected inside network [1]. That's why intrusion detection system (IDS) becomes an important research topic.

IoT paradigm quality makes it popular and has attracted massive industries, businesses' attention. These industries cover almost every field such like digital agriculture, autonomous vehicle, and many more [2]. Because of this technology, devices are enabling act smartly with intelligence. However, along with these advantages several security possibilities are also exists while illegitimate users tend to access IoT resources [3]. Threats emanating and IoT malware analysis by using texture features of images and various techniques of machine learning [4]. IoT along with IIoT (Industrial IoT) has developed speedily with privacy risks. Blockchain technology is a good approach to work on IoT device security issue [5]. Due to decentralized, persistency, and auditability properties, Blockchain technology have gained researchers attention [6].

In recent times, due to the emergence and popularity in society, various IoT definitions and many taxonomies have been presented [7]. IoT methodology includes objects connected in a network for collecting and exchanging data among each other via Internet [8]. As this communication often occurs in the public domain, it makes security attacks possible to IoT environment [8]. Cyber resilience identifies with cyber insurance and linked to the IoT which can simplify life using artificial intelligence [9].

Vision to develop IoT technology is to interconnect every object. This method enables smartness to objects by establishing communication among them. Along with smartness, unauthorized access vulnerability is also much higher [10]. To scrutinizes various malicious activities, methodology called intrusion detection by deep learning algorithms is used [10]. Implementation of dew computing in cyber-physical organizations allow smart and autonomous devices to collaborate and communicate with environment [11].

IoT linked with systems of computing devices, integrated objects, or machines in a network to exchange data without the presence of human [12]. In case of IoT networks, it is necessary to identify attack surface [12]. An integrated framework of cloud along with fog computing can be used to monitor smart traffic [13]. Smart home implementation is one of IoT major application and blockchain technology, can be deployed that start in the home gateway [14]. Fall diagnosis considers as a crucial aspect of a healthy life, so a powerful and emerging candidate called IoT used to develop a system for fall diagnosis [15]. Smart grid [16] technology face critical issue of high vulnerability towards cyber threads [16].

1.2. Contribution

State-of-art methods from the literature related to ML, IoT, and Blockchain are reviewed. This article tends to identify security issues in IoT and discuss recue possible by using ML and blockchain. Common definitions of IoT and different security issues are presented in this document. The severe intrusion problem that arises due to IoT devices connection to one another via the Internet. ML with its various approaches and blockchain technology is mentioned. The experiment has been conducted to detect intrusion by using learning approaches. The possibility for future research is also suggested.

1.3. Article Organization

Remainder part is structured into various sections. Section 2 mentions the relevant literature on IoT, its security issues, Machine Learning, and Blockchain. Next, section 3 explains IoT concept along with security requirements in IoT. Following, section 4 illustrates Blockchain technology. Section 5 elucidate Machine Learning along with its various approaches. Moreover, section 6 shows the experimental results to detect intrusion using various learning approaches. In addition, existing challenges and possibilities of this work for future is mentioned in this document section 7. Section 8 concludes all paperwork in its entirety.

2. Detailed Study

Due to IoT devices popularity and utility in a variety of domains, IoT industry has speedily grown. This section reviews and presents existing research related to IoT, its security concern, and possible solutions. The research relates to Machine Learning, and Blockchain has been also studied and presented in this section.

2.1. IoT and Security Issues

Elhadj et. al. [17] has concern with IoT intrusion detection systems and provides a critical review of IDS challenges for IoT. Further, this paper presents and evaluate future direction proposal in IDS based on IoT.

Along with benefits, IoT devices also come with serious security problem and privacy loss risk. Authors Ref. [18] perform a comprehensive survey of IoT devices and concern security issues and privacy loss. This survey has four parts. First part explores IoT devices limitations with their solutions. Next part mentions IoT attacks classification. To authenticate and for access control, the third part focused on the methods and architectures. On different layer security issue analyzed in the last part.

Paper authors Ref. [19] presents a detailed comprehensive survey of security techniques at the physical layer. This paper elaborates classification along with applications of security techniques at the physical layer for confidentiality.

IoT is next wave coming in society with the capability to revolutionize society and smart environment [20]. This paper classifies IoT devices to smart environments by using characteristics of network traffic. In this study, trade-offs in between performance, cost, and speed involved is discussed to deploy framework for classification in real-time.

Ismail et. al. [21] explains the security requirement in IoT, and also elaborates vulnerabilities, attacks, and possible countermeasure. Thereby, access to huge data is provided by IoT, this data collected by wireless sensor networks via Internet [21].

2.2. Blockchain

Mehran et. al. [22] discusses potential and efficient solution to solve forensic by using blockchain in SDN. Blockchain is a network of peers of distributed type which utilization can be on SDN based IoT to provision security. Blockchain technology is used to meet forensic challenges such like altering evidences, data integrity [22]. In order to address issues of detecting poor attacks along with slow processing, a forensics architecture called SDN-IoT is proposed.

The authors Ref. [23] elaborates blockchain and its role in industrial IoT (IIoT). This paper discusses various ongoing challenges, advances, and opportunities in reference to security and privacy. This study, then concludes peculiar issue with the various potential research plan.
In current scenario, IoT is an innovative technology effecting everywhere that makes its security essential and a crucial research challenge [24]. This paper provides a mathematical expression for calculating end-to-end delay with various network configurations [24]. Recently, blockchain is offering a good solution to diminish network limitations [24].
Pourush et. al. [25] describes IoT and blockchain. It explains this technology with respect to IoT applications. IoT defined as billions of devices interconnected in a network for communication. Security problems may arise, to overcome that blockchain technology is used in this paper.
Seoyun et. al. [26] discusses about IoT through which a hyper-connected society is created and IoT devices can cause a severe security concern. This paper [26] on the basis of blockchain for IoT devices proposes a distributed firmware update architecture.

2.3. Machine Learning

Sahrish et. al. [27] proposes a policy framework which is flow-based. This policy framework is based on two-tier virtualization and for vehicular networks by using SDN (Software Defined Networking). Motivation of study Ref. [27] is implementing an architecture which is machine learning-enabled in order to cater modern vehicular Internet infrastructure's sophisticated demands.
A comprehensive survey is conducted in study Ref. [28] on big data along with machine learning application in smart grid. This paper presents obtained key information from a literature review in tabular form in corresponding sections to give a complete and clear picture [28].
A sparse approach based on machine learning to recover and eliminate impulsive noise [29]. The result gets from computer simulation confirms that scheme proposed performs better than conventional methods [29].
IoT advancement is bringing advance intelligent commands on which societal daily life depends [30]. Paper Ref. [30] gives IoT and machine learning overview and works in intrusion detection. Existing mechanism of machine learning has been used for improving intrusions and cyber attacks [30].
Srinikethan et. al. [31] works to identify link fault with localization present in typical networks on the basis of ML. Performance of ML-LFIL gets high accuracy and low fault localization as compared with an active probing approach [31].

3. IoT Concept and Requirement of Security in IoT

IoT is a way to establish communication by connecting massive physical as well as virtual devices using Internet [32]. Because of IoT outstanding results, pace of Internet use and device connectivity is rapidly increasing. IoT applications has vast spectrum, all comes with security problem and issues of privacy. IoT architecture has several layers with some specific security threats. IoT architecture is also concerned with different objects like sensors, gateways, etc. Each layer has its own functioning. Various objects are associated with the respective IoT layer. It means that IoT architecture is divided into several IoT layers. All IoT layers have their

specific definition, and each layer consists of various objects, along with that, each layer has security threats. Due to connectivity between heterogenous devices via the Internet, large data are generated. It increases the surface for attack [32]. Thus, IoT devices needs careful security measures. Following Table 1 shows the various IoT layers, IoT layers' objects, and several possible security attacks [32],[33].

Table 1. IoT Layers, objects, and security threats

IoT Layers	Objects	Attacks Types
Sensing/Physical Layer	Sensors/Actuators	Injection of Malicious Code , Node Compromised Attack, Jamming Attack.
Network Layer	Internet, Gateways	Replay, Wormhole, Sybil, and Spoofing.
Application Layer	Edge IT	Software Modification, Reliability Attacks, Malicious Code.
Semantics Layer	Data Center/Cloud	Identity Theft, User Privacy Compromise.

Table 1 shows IoT layers, objects, and attack type possible on IoT. The description of various IoT layers is as follows [34]:

- IoT sensors or actuators are dealt with by the sensing layer. Sensors sense input and actuators perform action on the basis of sensory input data. To sense different data, different sensors like ultrasonic sensor, humidity sensor, etc. is present.
- Network Layer for processing transmits information to compute unit received from the previous sensing layer.
- Between the application and network layers is the middleware layer, which is an abstraction layer.
- Gateways Layer is also said as broad layer. It has the capability to connect devices, people, and cloud services. This layer performs encryption along with decryption of IoT data and protocol translation for communication in between various layers.
- The application layer is also termed as end-to-end layer. Direct dealing and providing services to end system user.

IoT devices have possibility of high vulnerability attack because of Internet use on a large scale for connectivity and communication [35]. This raise need of security for IoT devices with security objective called CIAA (Confidentiality, Integrity, Availability, Accountability) [35]. IoT security has aroused serious concern [36]. For IoT security, arbitrary detection of face occlusion can be used, in order to find crime behaviors [36]. To overcome IoT security issues, mechanisms of forensics as well as deep learning can be used [37]. To monitor the security of

mobile IoT on basis of machine learning along with processing of big data is possible [38]. In brief, requirement of security for the IoT devices is mentioned in Table 2 [39].

Table 2. Security requirement with various operational levels for IoT system

Operational levels	Security requirement	Definition
Information Level	Integrity	Received data should remain same.
	Anonymity	Hide data source identity from third party.
	Confidentiality	Third parties cannot read data.
	Privacy	Not disclose the private information of client at the time of data exchange.
Access Level	Access Control	Device access can be done by only legitimate users.
	Authentication	It checks the device right for network access. It also checks network right For device connection.
	Authorization	Ensures the authorized access.
Functional level	Resilience	It is network capacity for ensuring security.
	Self-organization	It is IoT system capability for adjusting itself to be operational.

Table 2 depicts a brief detail of IoT security requirement along with various operational levels [39]. Most popular and standard mechanisms for security are as follows:

- Encryption
- Lightweight cryptography
- Random number generator
- Secure hardware
- Intrusion Detection System

IoT domain is most exciting next revolution technology [40]. Security can be only barrier to success of this technology. Above-mentioned security mechanisms can be used to diminish this barrier. IoT cyber-security can be managed by using Machine Learning as well as a Programmable Telemetry [41]. Recently, IoT concept has been incorporated in smart cities

[42] and requirement of processing IoT data can be accomplished by using machine learning technology, especially SVM [42]. RF-PUF is a new technology that enhances IoT security for authentication like wireless nodes by using ML [43]. Location-based is crucial service in IoT to become intelligent system [44], that have to be secured and robust [44]. Thew heterogenous nature of IoT poses various security challenges, where testing becomes a complex task [45]. Nowadays, many cyber-attack challenges come because of IoT applications [46].
While IoT brings unprecedented efficiency, easy life style, and accessibility, IoT also has caused serious acute privacy and security issues [47]. “IoT features” [48] have high impact on severe issues of security and privacy [48].

Pervasive IoT growth is noticing world widely [48]. IoT security becomes most severe concern that needs special attention [48]. To secure IoT, detection of network intrusion is important and can be analyzed on the basis of learning techniques [48]. Analysis of IoT layers, protocols, and existing mechanism has paramount importance for securing communication [49]. Protection of communication in between IoT devices becomes an important issue for researchers [49].

4. IoT Security Solution using Blockchain Technology

The simplest way to describe blockchain is as a public distributed ledger system for protecting transaction records in environments of untrusted network [50]. A set of chained blocks in encrypted form is maintained by a blockchain node, where each node contains various transactions [50]. To check data integrity, role of blockchain nodes is same. Several common roles are as follows [50]:

- Receiving,
- Verifying, and
- Creating blocks

To check the IoT data integrity problem, the stochastic blockchain can be used [50]. IIoT stands for Industrial IoT that can be implemented using Resberry Pi and plays an important role, some of them are as follows [51]:

- Efficiency and security trade-off
- Transparency and privacy coexistence
- High accuracy v/s low throughput conflicts

Now, gradually IoT is becoming mature and plays an important role in daily life [52]. It helps to interconnect machines that make communication convenient and intellectual. Innumerable data produced by interconnected IoT devices require analyses in JointCloud. Because of IoT limitations, there are some problems exists in JointCloud, which are as follows:

- Trust Problems
- Privacy leakage concern
- IoT devices have weak security

As a trustworthy and promising tool, blockchain is able to solve excellently trust and privacy related problems [52]. However, above mentioned problems are still existing in IoT which can be handled by blockchain technology [52]. Nowadays, transportation system becomes more

intelligent that brings both new advance opportunities for vehicular IoT along with the challenges for VANETs (vehicular ad-hoc networks) [53]. Preserving user privacy and trust management, require a security scheme that should be reliable and practical. As the blockchain has immutable as well as decentralized characteristics, a security framework which is blockchain-based is designed for supporting services of vehicular IoT [53]. Without third party involvement, to establish mechanisms for trust along with consensus need blockchain in IoT [54]. Capability of blockchain technology to support trust and security transaction makes it more popular and widely used [55]. To mine using IoT, the blockchain becomes more decentralized as well as ubiquitous [55]. IoT is facing a significant problem of security challenges and scalability [56]. Due to this, IoT devices needs some external assistance [56]. Edge computing gives a direction to address centralized cloud computing deficiencies [56]. Latest emerging technologies, named blockchain as well as smart contracts, brings security features for both IoT as well as edge computing [56].

There are two types of blockchain networks, named permissionless, and permissions [56]. Bitcoin is a well-known example of permissionless blockchain, and EdgeChain system is an instance of permission [56]. The blockchain-based mechanism role for internet services are as follows [57]:

- Data security improvement to store personal content
- On the basis of consensus mechanism, a reliable scheme of incentive is provided
- For supporting internet services, scalability is provided

5. IoT Security Solution using Machine Learning

With Internet development, rapid and continuous growth in cyber-attacks also take place. Internet in-depth integration with social life, people living style changes. This also enhances serious security risk [58]. Artificial Intelligence successful branch named Machine Learning, basically work to make predictions using historical data and mathematical optimization [58]. For intrusion detection, approaches of machine learning can be applied [58]. Basic steps of machine learning models are as follows [58]:

- Feature Engineering
- Selection of suitable model of machine learning
- Model training
- Trained model to predict

IoT is continually getting pervasive growth and becoming famous world widely. With growth, IoT also brings severe security threads. Since, the success rate of machine learning has been good in security as well as in privacy. However, machine learning is a powerful technique in cyber security to detect intrusion [59]. Machine learning state-of-art techniques can be applied to analyze cognitive radios [60]. Nowadays, machine learning is most preferred and prevailing model in various recognition/classifying problems. Its widely used applications are such like image processing, intrusion detection, etc. [61]. It is also a good tool to work with tensor techniques [62]. Undoubtedly, machine learning is an important technique to endow intelligent functions in wireless network [63]. Currently, due to speed development of the Internet along with technologies of mobile communication, networking systems is becoming more and more

tedious and heterogenous that needs machine learning intelligence to analyze, organize the complex networking system [64],[65]. Recently, as technology proliferates, e-learning has also garnered with significant attention [66]. With growing data, analyses become important using machine learning [66]. Face recognition plays a vital role in many multi-disciplines researches such like computer science, neuroscience, and many others by conveying important information like race, gender, and much more [67]. These days, due to technology advancement, traffic classification becomes as an upcoming challenging problem [68]. A brief summary of well- known ML models is depicted in Table 3.

Table 3: Well-known learning approaches

Learning Approaches	Basic Meaning	Type of Problem	Benefits	Pitfalls	References
Naïve Bayes	A Machine Learning Technique used To classify data.	Classification.	Simple implementation, Easy to train Data	Difficult to Tackle continuous data. It relies The on independence assumption i.e. unrealistic.	[69]
Decision Tree	A model Of machine learning, basically for classification.	Classification, Regression	Simple to learn, Easy to understand, Easy rule extraction.	Instability, Over-fitting.	[70]
K Neighbors	Technique Of machine learning that classify Data based on K values.	Classification, Regression	Simple algorithm, Easy implementation, Free to select distance	Computationally expensive, Memory intensive.	[71],[72]

			function.		
Logistic Regression	A Machine learning famous approach To perform classification.	Classification	Simple approach, Easily understandable.	Tedious to Handle Hard problems.	[73],[74]

Table 3 shows a brief comparison of various well-known approaches of machine learning. In the next section, all learning models, mentioned in table 3 are compared and analyzed through experimental results. In order to detect intrusion, which is a serious problem, learning algorithm efficiency is compared in terms of accuracy. As IoT devices are interconnected via the Internet, intrusion detection becomes important with the purpose of security and to overcome loss of privacy risk.

6. Experimental Analysis using Machine Learning for Intrusion Detection

IoT technology removing distance barriers by interconnecting devices world widely via the Internet. However, it also brings severe security issues, which needs special attention. The intrusion detection problem has got paramount importance. This section uses intrusion detection dataset. This dataset is taken from Kaggle. This section uses various well- known algorithms of ML to detect intrusion. These algorithms brief description is shown in the previous section. In this section, each model is first evaluated and then validated on the network intrusion detection dataset. Following subsection 6.1 shows the evaluation result, then subsection 6.2 depicts the validation output, and final subsection 6.3 compares learning algorithm efficiency in terms of accuracy.

6.1 Learning Models Evaluation

Models evaluation results are represented below.

6.1.1 Naïve Bayes Classifier Model Evaluation

This model confusion matrix is as follows:

[[7000 1245]
[392 8997]]

Table 4 in the section below contains the classification report.

Table 4: Naïve Bayes Classifier Model Evaluation

	Precision	Support	F1-score	Recall
Anomaly	.95	8245	.90	.85
Weighted avg	.91	17634	.91	.91
Macro avg	.91	17634	.91	.90

Normal	.88	9389	.92	.96

6.1.2 Decision Tree Classifier Model Evaluation

This model confusion matrix is as follows:
[[8245 0]
[0 9389]]
The classification report is shown in Table 5.

Table 5: Decision Tree Classifier Model Evaluation

	Precision	Support	F1-score	Recall
Anomaly	1	8245	1	1
Weighted avg	1	17634	1	1
Macro avg	1	17634	1	1
Normal	1	9389	1	1

6.1.3 K Neighbors Classifier Model Evaluation

This model confusion matrix is as follows:
[[8168 77]
[33 9356]]

Table 6 in the section below contains the classification report.

Table 6: K Neighbors Classifier Model Evaluation

	Precision	Support	F1-score	Recall
Anomaly	1	8245	.99	.99
Weighted avg	.99	17634	.99	.99
Macro avg	.99	17634	.99	.99
Normal	.99	9389	.99	1

6.1.4 Logistic Regression Classifier Model Evaluation

This model confusion matrix is as follows:
[[7757 488]
[313 9076]]

Table 7 in the section below contains the classification report.

Table 7: K Neighbors Classifier Model Evaluation

	Precision	Support	F1-score	Recall
Anomaly	.96	8245	.95	.94
Weighted avg	.95	17634	.95	.95
Macro avg	.96	17634	.95	.95

Normal	.95	9389	.96	.97

6.2 Validation Models Evaluation

Models validation results are represented below.

6.2.1 Naïve Bayes Classifier Model Test Results

This model confusion matrix is as follows:

[[2981 517]
[188 3872]]

The classification report is shown in Table 8.

Table 8: Decision Tree Classifier Model Test Results

	Precision	Support	F1-score	Recall
Anomaly	.94	3498	.89	.85
Weighted avg	.91	7558	.91	.91
Macro avg	.91	7558	.91	.90
Normal	.88	4060	.92	.95

6.2.2 Decision Tree Classifier Model Test Results

This model confusion matrix is as follows:

[[3483 15]
[25 4035]]

Table 9 in the section below contains the classification report.

Table 9: K Neighbors Classifier Model Test Results

	Precision	Support	F1-score	Recall
Anomaly	.99	3498	.99	.99
Weighted avg	.99	7558	.99	.99
Macro avg	.99	7558	.99	.99
Normal	.99	4060	.99	.99

6.2.3 Logistic Regression Classifier Model Test Results

This model confusion matrix is as follows:

[[3298 200]
[136 3924]]

Table 10 in the section below contains the classification report.

Table 10: K Neighbors Classifier Model Test Results

	Precision	Support	F1-score	Recall
Anomaly	0.96	3498	0.95	0.94
Weighted avg	0.96	7558	0.96	0.96

Macro avg	0.96	7558	0.96	0.95
Normal	0.95	4060	0.96	0.97

6.3 Learning Models Efficiency (Accuracy) Comparison

This section shows comparison of various learning models in terms of accuracy. The accuracy gains during training and then in testing are presented and compared in following Table 11.

Table 11: Learning Models Efficiency Comparison

Learning Model	Training Accuracy	Testing Accuracy
Naïve Bayes Classifier	0.90716797096518	0.906721354855782
Decision Tree Classifier	1	0.994707594601746
K Neighbor Classifier	0.993762050584098	0.99166446149775
Logistic Regression	0.954576386526029	0.95554379465467

The following figure 2 pictorially shows the training accuracy and testing accuracy comparison.

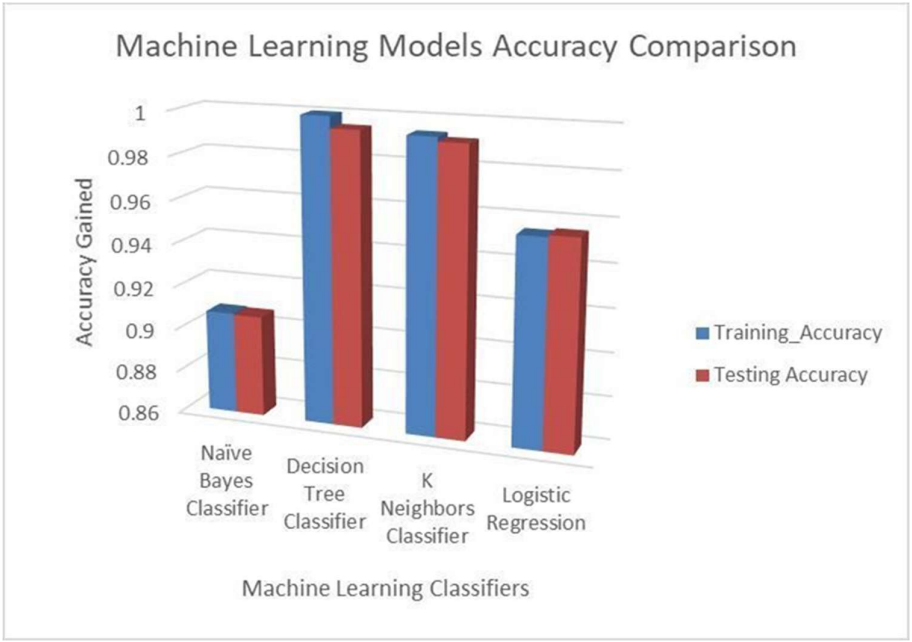

Figure 2 Learning Models Comparison

7. Existing Challenges with Future Trend

With the rapid growth of IoT, internet usage is also speedily increasing. Blockchain early development is influenced by main five internet technologies (Routers, TCP/IP, Web applications, information security technology, P2P). To tackle blockchain version 1.0 and 2.0 limitations, its third generation was proposed. However, several limitations still it has like smart contract security, consensus efficiency. Blockchain 4.0 is being presented and targets for improving consensus efficiency and thus tailoring blockchain to a future environment. Machine learning output improves with dataset size. The existing challenge is the availability of large correct data, so that machine can learn more accurately and can shows the good results in

intrusion detection and other application areas. Future research is possible by applying learning approaches on the large heterogenous dataset.

8. Conclusion

This paper concluded that IoT is a next wave revolutionary technique. Security could be only barrier in the path of success of this technology. This barrier can be positively handled by using blockchain and ML detection models. Nowadays, blockchain and machine learning both are the high privileged and most advanced technologies. This paper elaborates IoT and its uprising demand in society. This study also illustrates security and privacy challenge faced by this technology. Further, this document explains blockchain methodology and its purpose to overcome security challenge. Machine learning and its models gain success in a number of applications. Here, this article experimentally analyzes learning approaches using network intrusion detection dataset.

References

1. Casola, V., De Benedictis, A., Riccio, A., Rivera, D., Mallouli, W., & de Oca, E. M. (2019). A security monitoring system for internet of things. Internet of Things, 7, 100080.
2. HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 100129.
3. Mbarek, B., Ge, M., & Pitner, T. (2020). An Efficient Mutual Authentication Scheme for Internet of Things. Internet of Things, 100160.
4. Karanja, E. M., Masupe, S., & Jeffrey, M. G. (2020). Analysis of internet of things malware using image texture features and machine learning techniques. Internet of Things, 9, 100153.
5. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2019). Blockchain for the IoT and industrial IoT: A review. Internet of Things, 100081.
6. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. Internet of Things, 100107.
7. Alkhabbas, F., Spalazzese, R., & Davidsson, P. (2019). Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. Internet of Things, 7, 100084.
8. Zeadally, S., Das, A. K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. Internet of Things, 100075.
9. Hausken, K. (2020). Cyber Resilience in Firms, Organizations and Societies. Internet of Things, 100204.
10. Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2019). Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet of Things, 100112.
11. Lakkadi, S., Mishra, A., & Bhardwaj, M. (2015). Security in ad hoc networks. American Journal of Networks and Communications, 4(3-1), 27-34.
12. Jain, Ishita and Bhardwaj, Dr. Manish, A Survey Analysis of COVID-19 Pandemic Using Machine Learning (July 14, 2022). Proceedings of the Advancement in Electronics &

Communication Engineering 2022, Available at SSRN: https://ssrn.com/abstract=4159523 or http://dx.doi.org/10.2139/ssrn.4159523
13. Sharma, A., Tyagi, A., & Bhardwaj, M. (2022). Analysis of techniques and attacking pattern in cyber security approach: A survey. International Journal of Health Sciences, 6(S2), 13779–13798. https://doi.org/10.53730/ijhs.v6nS2.8625.
14. Gushev, M. (2020). Dew Computing Architecture for Cyber-Physical Systems and IoT. Internet of Things, 100186.
15. Rizvi, S., Orr, R. J., Cox, A., Ashokkumar, P., & Rizvi, M. R. (2020). Identifying the Attack Surface for IoT Network. Internet of Things, 100162.
16. Dhingra, S., Madda, R. B., Patan, R., Jiao, P., Barri, K., & Alavi, A. H. (2020). Internet of things-based fog and cloud computing technology for smart traffic monitoring. Internet of Things, 100175.
17. Minoli, D. (2019). Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. Internet of Things, 100147.
18. Mozaffari, N., Rezazadeh, J., Farahbakhsh, R., Yazdani, S., & Sandrasegaran, K. (2019). Practical Fall Detection Based on IoT Technologies: A Survey. Internet of Things, 100124.
19. Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R. M., & Srivastava, G. (2019). Security aspects of Internet of Things aided smart grids: a bibliometric survey. Internet of Things, 100111.
20. Benkhelifa, E., Welsh, T., & Hamouda, W. (2018). A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE Communications Surveys & Tutorials, 20(4), 3496-3509.
21. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250-1258.
22. Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2018). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), 1773-1828.
23. Tyagi, A., Sharma, A., & Bhardwaj, M. (2022). Future of bioinformatics in India: A survey. International Journal of Health Sciences, 6(S2), 13767≤13778. https://doi.org/10.53730/ijhs.v6nS2.8624.
24. Chauhan, P., & Bhardwaj, M. (2017). Analysis the Performance of Interconnection Network Topology C2 Torus Based on Two Dimensional Torus. International Journal of Emerging Research in Management &Technology, 6(6), 169-173.
25. Pourush, N. S., & Bhardwaj, M. (2015). Enhanced Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. American Journal of Networks and Communications, 4(3), 25-31.
26. Sivanathan, A., Gharakheili, H. H., Loi, F., Radford, A., Wijenayake, C., Vishwanath, A., & Sivaraman, V. (2018). Classifying IoT devices in smart environments using network traffic characteristics. IEEE Transactions on Mobile Computing, 18(8), 1745-1759.
27. Butun, I., Österberg, P., & Song, H. (2019). Security of the internet of things: vulnerabilities, attacks and countermeasures. IEEE Communications Surveys & Tutorials.

28. Pourvahab, M., & Ekbatanifard, G. (2019). An efficient forensics architecture in software-defined networking-IoT using blockchain technology. IEEE Access, 7, 99573-99588.
29. Wu, J., Haider, S. A., Bhardwaj, M., Sharma, A., & Singhal, P. (2022). Blockchain-Based Data Audit Mechanism for Integrity over Big Data Environments. Security and Communication Networks, 2022.
30. Bhardwaja, M., & Ahlawat, A. (2019). Evaluation of Maximum Lifetime Power Efficient Routing in Ad hoc Network Using Magnetic Resonance Concept. Recent Patents on Engineering, 13(3), 256-260.
31. Bhardwaj, M., & Ahalawat, A. (2019). Improvement of Lifespan of Ad hoc Network with Congestion Control and Magnetic Resonance Concept. In International Conference on Innovative Computing and Communications (pp. 123-133). Springer, Singapore.
32. Bhardwaj, M., & Ahlawat, A. (2017). Optimization of Network Lifetime with Extreme Lifetime Control Proficient Steering Algorithm and Remote Power Transfer. DEStech Transactions on Computer Science and Engineering.
33. Choo, K. K. R., Yan, Z., & Meng, W. (2020). Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges and Opportunities. Ieee Transactions on Industrial Informatics, 16(6), 4119-4121.
34. Alaslani, M., Nawab, F., & Shihada, B. (2019). Blockchain in IoT Systems: End-to-End Delay Evaluation. IEEE Internet of Things Journal, 6(5), 8332-8344.
35. Viriyasitavat, W., Da Xu, L., Bi, Z., & Hoonsopon, D. (2019). Blockchain Technology for Applications in Internet of Things—Mapping From System Design Perspective. IEEE Internet of Things Journal, 6(5), 8155-8168.
36. Choi, S., & Lee, J. H. (2020). Blockchain-Based Distributed Firmware Update Architecture for IoT Devices. IEEE Access, 8, 37518-37525.
37. Tayyaba, S. K., Khattak, H. A., Almogren, A., Shah, M. A., Din, I. U., Alkhalifa, I., & Guizani, M. (2020). 5G Vehicular Network Resource Management for Improving Radio Access Through Machine Learning. IEEE Access, 8, 6792-6800.
38. Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of big data and machine learning in smart grid, and associated security concerns: A review. IEEE Access, 7, 13960-13988.
39. Liu, S., Xiao, L., Huang, L., & Wang, X. (2019). Impulsive Noise Recovery and Elimination: A Sparse Machine Learning Based Approach. IEEE Transactions on Vehicular Technology, 68(3), 2306-2315.
40. Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine Learning for Security and the Internet of Things: the Good, the Bad, and the Ugly. IEEE Access, 7, 158126-158147.
41. Srinivasan, S. M., Truong-Huu, T., & Gurusamy, M. (2019). Machine Learning-Based Link Fault Identification and Localization in Complex Networks. IEEE Internet of Things Journal, 6(4), 6556-6566.
42. Bhardwaj, M., & Ahlawat, A. (2017). Enhance Lifespan of WSN Using Power Proficient Data Gathering Algorithm and WPT. DEStech Transactions on Computer Science and Engineering.

43. Megha Sharma, Shivani Rohilla, Manish Bhardwaj, Efficient Routing with Reduced Routing Overhead and Retransmission of Manet, American Journal of Networks and Communications. Special Issue: Ad Hoc Networks. Volume 4, Issue 3-1, May 2015 , pp. 22-26. doi: 10.11648/j.ajnc.s.2015040301.15
44. Bhardwaj, M. (2020). 7 Research on IoT Governance, Security, and Privacy Issues of Internet of Things. Privacy Vulnerabilities and Data Security Challenges in the IoT, 115.
45. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2018). Anatomy of threats to the internet of things. IEEE Communications Surveys & Tutorials, 21(2), 1636- 1675.
46. Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data collection for security measurement in wireless sensor networks: a survey. IEEE Internet of Things Journal, 6(2), 2205-2224.
47. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
48. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), 2702-2733.
49. Mao, L., Sheng, F., & Zhang, T. (2019). Face Occlusion Recognition With Deep Learning in Security Framework for the IoT. IEEE Access, 7, 174531-174540.
50. Koroniotis, N., Moustafa, N., & Sitnikova, E. (2019). Forensics and deep learning mechanisms for botnets in Internet of Things: A survey of challenges and solutions. IEEE Access, 7, 61764-61785.
51. Kumar, A., Rohilla, S., & Bhardwaj, M. (2019). Analysis of Cloud Computing Load Balancing Algorithms. International Journal of Computer Sciences andEngineering, 7, 359-362.
52. Bhardwaj, M., Ahlawat, A., & Bansal, N. (2018). Maximization of Lifetime of Wireless Sensor Network with Sensitive Power Dynamic Protocol. International Journal of Engineering & Technology, 7(3.12), 380-383.
53. Bhardwaj, M. and Ahlawat, A. (2018) Wireless Power Transmission with Short and Long Range Using Inductive Coil. Wireless Engineering and Technology, 9, 1-9. doi: 10.4236/wet.2018.91001.
54. Kotenko, I., Saenko, I., & Branitskiy, A. (2018). Framework for mobile Internet of Things security monitoring based on big data processing and machine learning. IEEE Access, 6, 72714-72723.
55. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. IEEE Internet of Things Journal, 6(5), 8182-8201.
56. Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, Q. Z. (2016). IoT middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal, 4(1), 1- 20.
57. Sivanathan, A., Gharakheili, H. H., & Sivaraman, V. (2020). Managing IoT cyber-security using programmable telemetry and machine learning. IEEE Transactions on Network and Service Management, 17(1), 60-74.

58. Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things Journal, 6(5), 7702-7712.
59. Chatterjee, B., Das, D., Maity, S., & Sen, S. (2018). RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning. IEEE Internet of Things Journal, 6(1), 388-398.
60. Chen, L., Thombre, S., Järvinen, K., Lohan, E. S., Alén-Savikko, A., Leppäkoski, H., ... & Lindqvist, J. (2017). Robustness, security and privacy in location-based services for future IoT: A survey. IEEE Access, 5, 8956-8977.
61. Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., ... & Elovici, Y. (2019). Security testbed for internet-of-things devices. IEEE Transactions on Reliability, 68(1), 23-44.
62. Li, F., Shinde, A., Shi, Y., Ye, J., Li, X. Y., & Song, W. (2019). System statistics learning-based IoT security: Feasibility and suitability. IEEE Internet of Things Journal, 6(4), 6396-6403.
63. Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606-1616.
64. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.
65. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.
66. Chen, Y. J., Wang, L. C., & Wang, S. (2018). Stochastic Blockchain for IoT Data Integrity. IEEE Transactions on Network Science and Engineering.
67. Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), 3680-3689.
68. Yang, H., Yuan, J., Yao, H., Yao, Q., Yu, A., & Zhang, J. (2019). Blockchain-based hierarchical trust networking for jointcloud. IEEE Internet of Things Journal, 7(3), 1667-1673.