Chapter 13
Adversarial Artificial Intelligence Assistance for Secure 5G-Enabled IoT

Mohammed Husain Bohara, Khushi Patel, Atufaali Saiyed, and Amit Ganatra

1 Introduction

With the advancement of various technologies and increased capability of communication technologies, many things in terms of computing devices are connected with each other. Today, the Internet of Things (IoT) plays a major role to provide a comfortable and easier lifestyle to human beings by physically connecting sensors and other embedded devices. Moreover, machine learning (ML) and artificial intelligence (AI) add intelligence and self-learning capabilities in machines which significantly attract many users and devices to get connected with the Internet which significantly affects the automation of industry [1]. The globally connected IoT devices generate billions of data on a daily basis which can be used for training the models through machine learning techniques to incorporate intelligence with devices. By applying various AI techniques to the large amount of data generated by various IoT sensors, more automated IoT devices can be designed [1]. The expansion of big data and, recently, the applications of AI technologies in different fields have expanded rapidly. In object detection, image recognition, computer translation, speech control, and more advanced areas such as drug structure analysis, due to high intelligence, high availability, and high performance,

M. H. Bohara (✉) · K. Patel · A. Saiyed · A. Ganatra
Devang Patel Institute of Advance Technology & Research (DEPSTAR), Faculty of Technology and Engineering (FTE), Charotar University of Science & Technology (CHARUSAT), Changa, Gujarat, India
e-mail: mohammedbohara.ce@charusat.ac.in; khushipatel.ce@charusat.ac.in; saiyedatufaali.ce@charusat.ac.in; amitganatra.ce@charusat.ac.in

S. Tanwar (ed.), *Blockchain for 5G-Enabled IoT*,
https://doi.org/10.1007/978-3-030-67490-8_13

artificial intelligence technologies have been applied. Moreover, deep learning (DL) is attracting many industries in the field of computer vision to add momentum to AI-based applications. However, AI and ML with IoT are the most revolutionary technologies today; security concerns become the center of attraction for the major researchers.

Conventionally, the data with identical statistical parameters are used to train and deploy the ML models with a benign environment which is vulnerable to tampering of statistical parameters of the ML model by some capable intruder that leads to incorrect prediction. Some recent studies have indicated the neural networks are open to malicious attacks, current research on adversarial technology of artificial intelligence has slowly become a hotspot, and studies have regularly proposed new methods of adversarial attacks and methods of protection.

The adversarial attacks can be divided into three classes as per the target model's different phases: attacks in the training phase, attacks in the testing phase, and attacks in the model's implementation phase. Presently, artificial intelligence has several different sub-fields, such as intelligent optimization, biomedical devices, and machine learning [2, 3]. Here, the machine learning (ML) sub-field utilizes the learning mechanism which makes it the artificial intelligence's major sub-field. A typical method of machine learning uses certain metrics, which are knowledge and practical adjustment according to a set of target data, if previously obtained or evaluated instantly. It is for that reason the machine learning background is highly associated with statistics, mathematics, and logic [4, 5]. It is important that all the context provides machine learning with both certain benefits and drawbacks. Essential benefits for even modern, complex real-world problems are becoming versatile and simple to use. Alternatively, drawbacks include needing thorough review of the data, often using training phase for the data, and often needing reliable expertise for the true modeling for the problem. As with cyber security threats, today's and future intelligent systems can employ some gaps that make them vulnerable against attacks built with a powerful logical and mathematical context.

The Internet of Things (IoT) connects various things (sensors, actuators, etc.) with each other using communication technologies like the fifth generation (5G) to fulfill the demand of latency-sensitive applications. The data generated by various sensors with some identical parameters are provided to the ML models for training and deployment under some benign settings to make some decisions. The ML requires the reliable, trusted, and secure platform of data storage for working more effectively. The security and privacy of the data collected from the sensors during transmission and building the model using ML techniques plays an important role. Blockchain is a trusted and distributed ledger which provides integrity, resilience, and tamper-proof environment. Integration of such technologies like 5G (networking), Internet of Things (IoT), machine learning (ML), big data analytics (BDA), blockchain technology (BT), etc. plays a significant part in the revolution of automation in industry with a transparent environment.

1.1 Motivation

The motivation comes with the integration of IoT, blockchain, and machine learning. 5G is evolving to enhance the performance, security, and connectivity in IoT device. The 5G network targets to support the application of IoT. Blockchain can be used to solve the challenges of 5G-enabled IoT. Various concepts of blockchain with IoT are explored in the papers; some of the papers give brief ideas about the adversarial effects of machine learning. The data generated with the IoT devices can be trained with the machine learning models.

1.2 Contribution of This Survey

This chapter provides the detailed understanding about role of blockchain and 5G technology in integration of IoT and AI.

1. The evolution of blockchain technology with its architecture, types, and features is covered in this chapter.
    - The 5G offers numerous benefits to the IoT applications in terms of performance, fault tolerance, and decentralization. The overview of 5G-enabled IoT with the use of blockchain technology is covered.
    - The research in the area of adversarial attacks and types of adversarial attacks on machine learning models is in trend. The various examples of adversarial attacks, threat landscape, and their impacts are covered in detail. Various adversarial effects of machine learning techniques while the same set of parameters for the data is used for training and deploying the model are also covered.
    - The way of offering trustworthy machine learning approach to industry has been analyzed.
    - The various scenarios of integration of blockchain with IoT, 5G-enabled IoT, and AI along with their challenges and opportunities are covered.

1.3 Organization

The chapter structure is as follows: In Sect. 2, the basic theory of blockchain, evolution of blockchain, and types of blockchain with blockchain framework are explored. In Sect. 3, 5G-enabled IoT with architecture and use case of 5G-enabled IoT in blockchain is discussed. Section 4 explains various adversarial effects of machine learning techniques while the same set of parameters for the data is used for training and deploying the model. Blockchain technology is one of the trending

solutions for providing an immutable decentralized environment for data storage and transactions which can be utilized to provide a secure, trusted, and reliable environment to ML models for solving the adversarial effects. In the next section, the basics of blockchain technology, 5G communication, IoT, and adversarial AI techniques are covered. In Sect. 5, the threat landscape and how a trustworthy machine learning approach can be offered to industry are covered. Section 6 covers the attacks. Section 7 covers the role of blockchain in establishing trust among various parties in the machine learning model for industrial automation with the case study and challenges.

2 Background Theory

In this section, blockchain technology along with 5G-enabled IoT is covered to understand how to provide security against adversarial effects on machine learning and artificial intelligence (AI) models.

2.1 Blockchain Technology

The digital currency Bitcoin [6] which is based on blockchain is the first application of blockchain published in 2009 by a person named Satoshi Nakamoto. Blockchain was initially put forward as an underlying technical framework of Bitcoin. Due to excessive fluctuation and regulatory management, Bitcoin was deprived in many countries. The reason for the acceptance of blockchain by the public is the three security measures of confidentiality, reliability, and integrity. The era of Bitcoin was Blockchain 1.0.

The blockchain is an emerging area. In Fig. 13.1, the evolution of blockchain from 1.0 to 4.0 is depicted. The introduction of smart contracts in blockchain was the evolution of Blockchain 2.0. The smart contract is the set of instructions which can be configured in such a way that it gets executed automatically by miners on the occurrence of some event. Smart contract is used in Ethereum which is another well-known cryptocurrency. Nowadays, many industries get attracted toward developing various platforms for smart contracts which leads to adoption of smart contracts in various areas like ML, AI, IoT, and big data analytics for integration of blockchain.

Fig. 13.1 Evolution of blockchain technology from Bitcoin to blockchain in Industry 4.0

Fig. 13.2 Type of blockchain

Blockchain is used to transmit the data and transfer of data is done in a decentralized manner, without the involvement of any third party. From cryptocurrency to the numerous industries, blockchain is growing day by day. The blockchain provides the technical solution for the verification, authentication, and data storage. The blockchain is used in many applications such as financial market, voting system, IoT, medical, supply chain, and agriculture.

Today the blockchain is a trending technology. The data transfer is efficient using blockchain technology. Privacy is maintained using blockchain, and the trust of different parties increased, as it reduces the chance of victimization and provides the record of transaction done. Blockchain reduces the risk when the untrusted parties come into the finance business which generates the reliability. Using the Internet, we can transfer the data, image, movies, etc. in any corner of the world. Similarly, in the transaction, the sender trusts the unknown party and makes the transaction. But in the blockchain security is ensured for the transaction. Block in the blockchain transactions is recorded, and the time of the creation and modification of the block is also recorded.

The blockchain network can be categorized into different categories on the basis of access to the network which is permissionless and permissioned. Permissioned blockchain network is only accessible to authorized users in consortium or cloud-based environments, while permissionless blockchain is open for all the users. Figure 13.2 shows the various types of blockchain network.

Private and public blockchain are the types of blockchain. The classification is based on the access control, data storage, and parameters. In the public blockchain, any node can participate in the process, but in the case of private blockchain, the restriction is provided, and to enter the process, approval is required. Consortium blockchain falls under the category of permissioned blockchain but multiple organizations are involved.

2.2 Blockchain Framework

The blockchain is considered as the link of block data forming a chain-like structure; the representation of blockchain framework is explained in detail as shown in Fig. 13.3. The blockchain framework is divided into data link layer, network layer, and

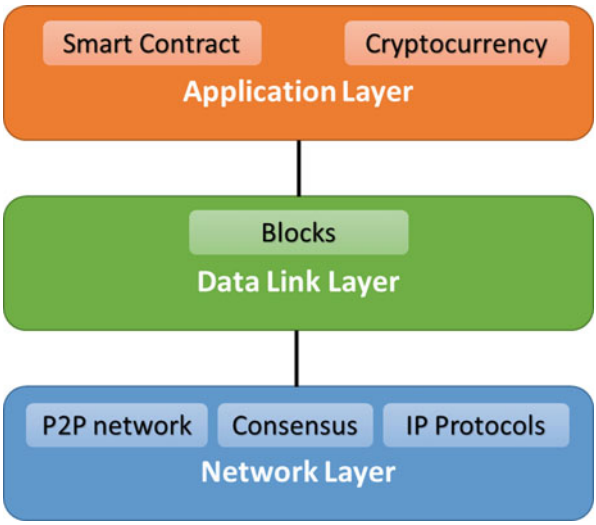

Fig. 13.3 Blockchain framework

application layer. In the data link layer, the block is created which includes the data structure, hash, Merkle root tree, and hash pointer. The network layer is used to interact with the blockchain which includes P-P network protocol and consensus algorithm. The network layer also enables the network distribution among the users. Lastly, the application layer integrates the blockchain with the application that enables the smart contact, Hyperledger, etc.

Blockchain is the technology that combines different algorithms, cryptography, and distributed networks. The blockchain works on the principle of the agreement of transaction without any central authority. In the blockchain, the blocks are linked to one another, and each block is linked with the hash of the block at the time stamp. The hash value is generated to verify the identity of the block.

3 5G-Enabled IoT

The Internet of Things, commonly referred to as IoT, connects the Internet with the electronic devices of different capabilities and structures. This is mainly done by wireless sensor, RFID, machine to machine, and Zigbee. The IoT comprises five components which are sensor, computing node, receiver, actuator, and device. To improve the efficiency of the system, the limitation with the usage of IoT needs to be resolved. Due to the increase in the usage of IoT devices, there should be a large amount of data transmission support with high bandwidth.

IoT is the technology to set the vision of connected living. It is not only to enhance the quality of life but new revenue generation. Capabilities of IoT promise to save people's and organizations' money and time while at the same time contributing toward enhanced outcomes in a wide range of novel application

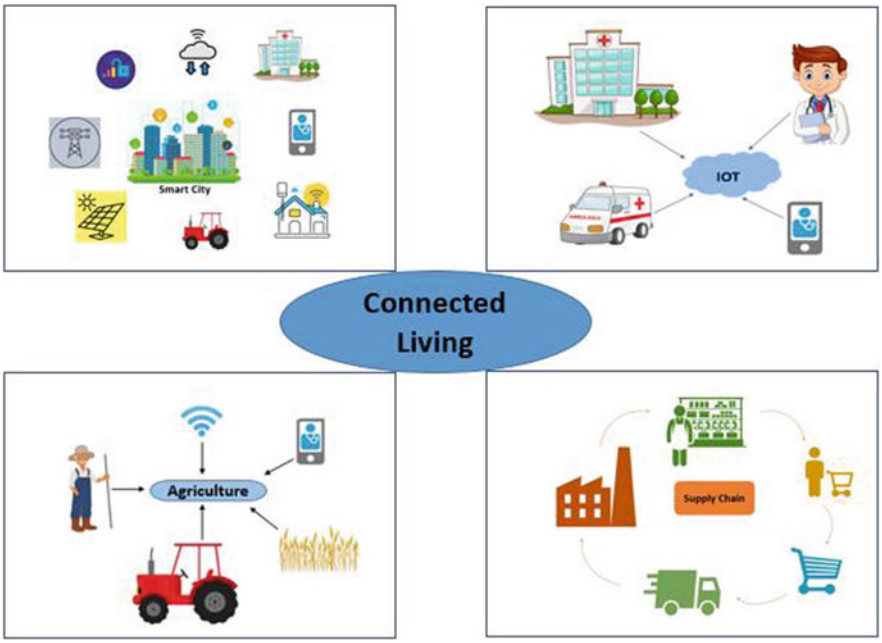

Fig. 13.4 IoT with connected living [8]

areas. The new era of living in the different areas like healthcare, smart city, agriculture, smart homes, etc. connects with IoT as shown in Fig. 13.4. The lifestyle would connect to IoT-enabled devices with the various applications. The advance of wireless technology which is the fifth-generation wireless systems (5G) is a driver for the 5G-enabled IoT applications. Next-generation 5G is rapidly growing as the massive machine-type communication transfers to high-level 5G technology. This would lead to IoT with 5G technology.

5G is evolving to enhance the performance, security, and connectivity in IoT device. The 5G network can provide faster speed than any other generation. In the past years, many researches have been done. The CISCO, Intel, and Verizon have jointly worked upon a research project on 5G and designed a novel set of "neuroscience-based algorithms" that adapt video quality to the demands of the human eye, suggesting that the future wireless networks would have built in human intelligence [7].

3.1 5G IoT Architecture

During each phase, 5G IoT is expected to provide end-to-end data transfer with real-time applications. The architecture provides independent network and use of

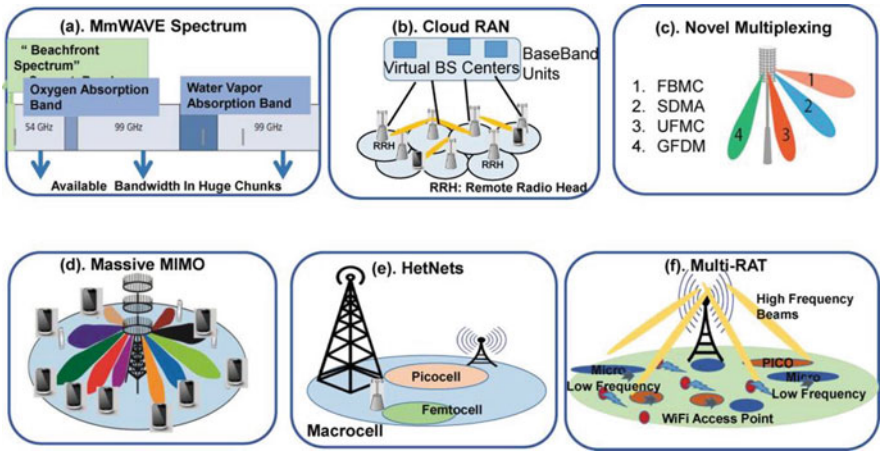

Fig. 13.5 5G-enabled IoT [8]

cloud-based radio access network (CloudRAN) to provide on-demand deployment of the applications. 5G required some key enabling technologies such as high bandwidth, high battery life – fundamental requirement in 5G, flexible and novel time-frequency multiplexing, antenna array technology for narrowband operation, HetNets, and massive MIMO for IoT architecture, network virtualization, self-organizing network (SON), and coexistence of multiple radio access.

3.2 Use of 5G-Enabled IoT in Blockchain

Cloud computing is the centralized data storage system and is used in the development of IoT. But the issue in cloud computing is data privacy. The user is not aware about where the data is stored in the network. Therefore, such systems fail to meet the requirement of the user. To secure the data and maintain the privacy, blockchain is the efficient solution. Blockchain has the ability to revolutionize IoT with an open, trusted, and auditable sharing platform, where any information exchanged is reliable and traceable. Some of the benefits of this integration are as shown in Fig. 13.5 [9].

4 Adversarial Artificial Intelligence

In this section, we present mainly adversarial samples and types of attack, including the causes and features of adverse samples and the capabilities and objectives of the adversarial attacks.

Here we define the common technical terms relating to adversarial machine learning attacks.

- *Adversary* – More commonly, adversary refers to the operator who produces an example of adversity.
- *Adversarial Attack* – Current research incorporates techniques on machine learning and deep learning for adversarial attacks. This deals fundamentally with the concept of fooling train models.
- *Adversarial Example* – It is a changed version of a data cleansing that purposefully adds noise to confuse a model of machine learning.
- *Adversarial Training* – Apart from the clean data, adversarial training uses adversarial data set to build machine learning models.
- *Black-Box Attack* – A type of attack that feeds adversarial examples to a specific model which are created without that model's awareness.
- *Threat Model* – The model of threat refers to different types of potential attacks which a strategy considers, e.g., black-box attack.
- *White-Box Attack* – An attack that presumes the full understanding of the target model, including its values for parameters, design, training process, and in some cases even training data.

4.1 Types of Attack

In this section, we are going to explain a few attacks with examples for better understanding of the topic.

4.1.1 Box-Constrained L-BFGS

The authors in [10] first show the existence of minor disruptions to the photos, so the disrupted photos could trick the classification errors of deep learning models. These contradictory findings have thus provoked a wide interest among researchers in the area of computer vision adversarial assaults using deep learning (Fig. 13.6).

4.1.2 Fast Gradient Sign Method (FGSM)

Szegedy et al. [10] found that adversary training could increase the robustness of deep neural networks against the adversarial instances. Goodfellow et al. [12] introduced a strategy for efficiently calculating an adversarial disturbance for a given image in order to allow effective adversarial training. The Python program in [13] tricks the regression model as the method of target machine learning (full source code can be downloaded from the GitHub folder of the developer:

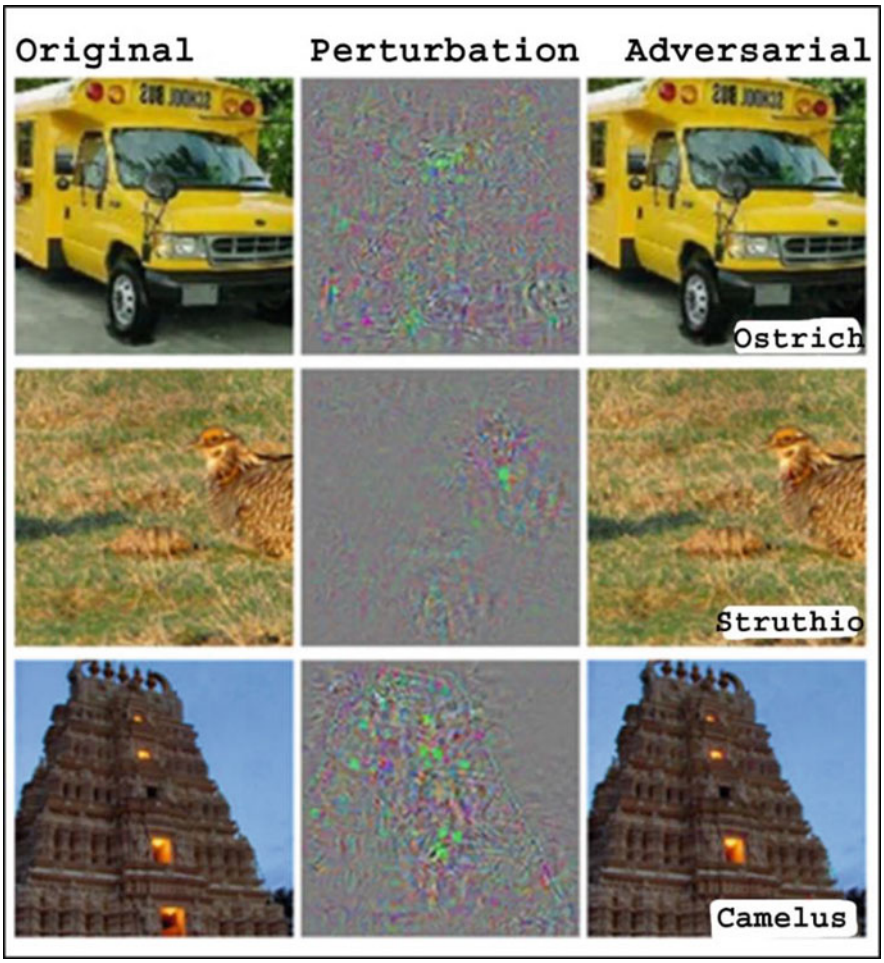

Fig. 13.6 Examples of adversarial created using AlexNet [10, 11]

https:/github.com/kenhktsui/adversarial examples). As can be seen from Fig. 13.7, the true data was categorized by the regression analysis into two groups.

4.1.3 One-Pixel Attack

An intense attack scenario on the opponent is when just a single pixel is modified in the picture to deceive the classifier. Su et al. [14] confirmed that three different types of neural network models were successfully fooled on 70–97 percent of the images tested by only changing a single pixel in each frame. Figure 13.8 shows that every image contains the appropriate label, and the resulting predicted label is shown in brackets.

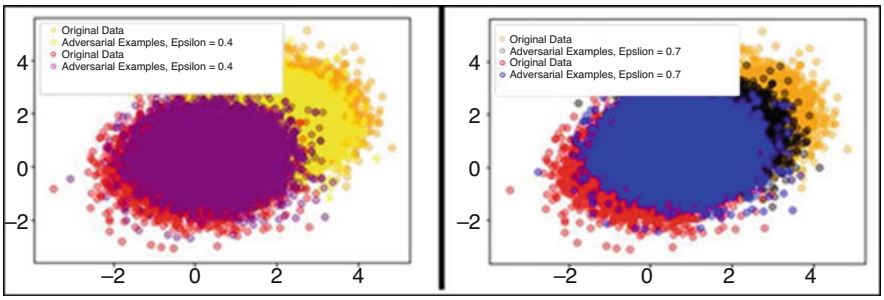

Fig. 13.7 Actual classification outputs and erroneous classifications for two distinct 0.4 and 0.7 epsilon values, respectively (as stated by Tsui in [13] application)

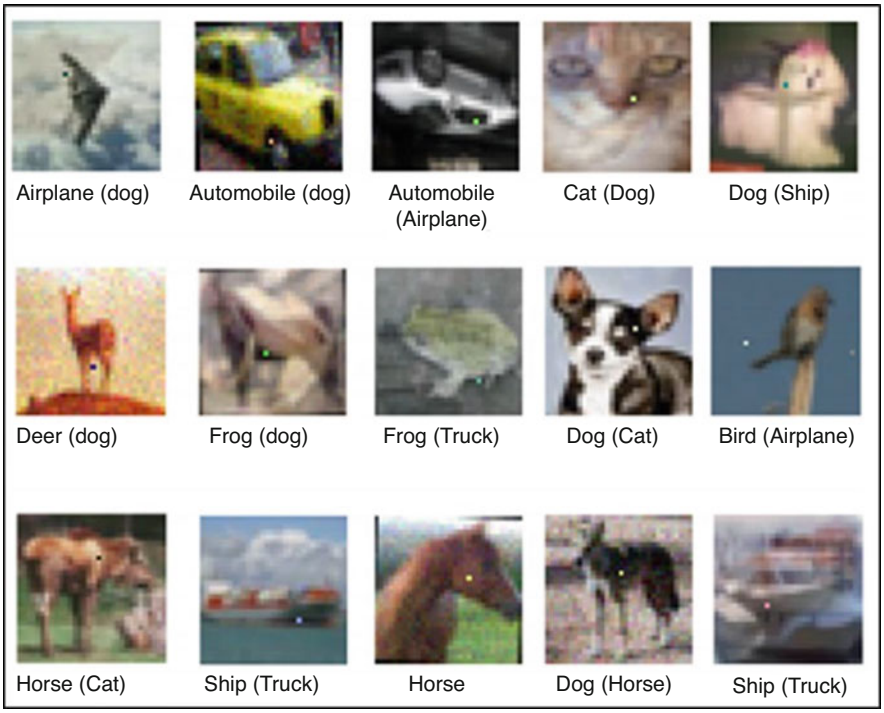

Fig. 13.8 Single-pixel adversarial attacks [14]

4.1.4 Carlini and Wagner Attacks (C&W)

In the wake of defensive distillation against the adversarial perturbations, Carlini et al. [15] introduced a set of three adversarial attacks [16] (Fig. 13.9).

Corresponding code for Nicholas Carlini and David Wagner's paper "Towards Evaluating the Robustness of Neural Networks," presented at

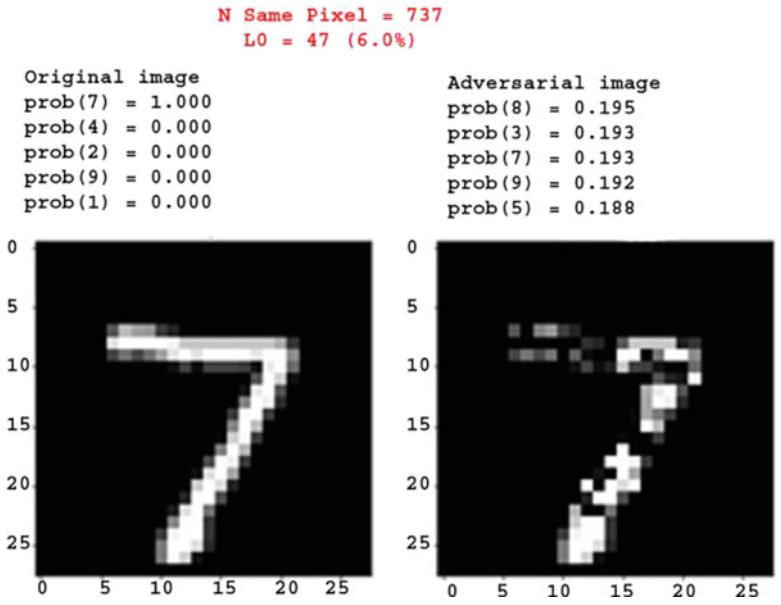

Fig. 13.9 Carlini and Wagner's adversarial attack on MNIST [15]

the IEEE Security and Privacy Symposium, 2017 is available online at https://github.com/carlini/nn_robust_attacks.

4.1.5 DeepFool

Dezfooli et al. [17] suggested iteratively calculating a minimum standard of adversarial disturbance for an input image. Their technique, that is, DeepFool, initializes the clean picture presumed to be located in an area confined to classifier decision limits.

5 Trustworthy Machine Learning for Industry

Breakthroughs in computational capacity have made online quantitative machine learning a useful and practical tool in many systems and networking domains to solve decision-making problems, spam filtering, virus detection, and network intrusion detection. A machine learning algorithms such as a support vector machine (SVM) and Bayesian learner can be useful in these domains [18].

5.1 Machine Learning Technique and Issues

In actual life, people are really going to classes, learning from lessons, and trying to offer some tests to show they've learned something right. Similarly, the machine learning techniques' pre-learning phase is performed along with training data, and few other databases have been used to check whether the model has been properly trained [19]. Because machine learning's logical and mathematical architecture will cause regularization, it means to remember the data pattern. In that case, the method is not effective because it has merely been memorized. It's similar again for the learning cycle of humans as if we remember something, it can be successful in the short term but it doesn't mean we're going to pass the main exam. When a machine learning approach works in the testing process as well, then it can be approved to be implemented in actual applications. Basically, it can be said for all machine learning techniques the process involves the "reading," "testing," and "download" phases (Fig. 13.10a) [20].

Some important issues in machine learning are data for learning and shaping the target problem. It is also essential to choose the most effective approaches for machine learning, as some mechanisms may not be successful on specific problems. Moreover, because machine learning techniques may use their own required features, selecting the most suitable value for these parameters is another problem. Eventually, some other problems that should be addressed are the total iterative process number for improved learning or a data preprocessing step for information collected (Fig. 13.10b) [20].

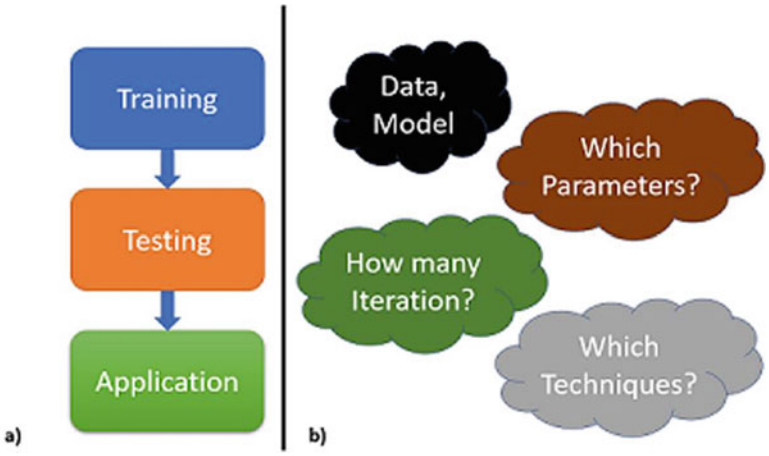

Fig. 13.10 (**a**) Machine learning cycle. (**b**) Machine learning issues [20]

5.2 *Learning Paradigms*

Data obtained from the different sources may not all be in the similar form, although the ML algorithm uses various learning steps to make them ready for use. At present, there are three different learning paradigms that can be defined as follows.

5.2.1 Supervised Learning

It is a type of learning process, where results are identified for each individual data input. In these, each given set of input cases is labeled with known target output classes for the problem under consideration, which means that a successfully trained model with supervised learning can forecast a result and also classify according to a newly discovered combination of inputs. Figure 13.11 reflects traditional (a) mathematical and visual regression and (b) nonlinear classification [21, 22].

5.2.2 Unsupervised Learning

Unsupervised learning occurs when results are not identified for the target data from which to learn. Basically, it calculates similitudes-distances between gathered data and group them into a certain similar number of clusters. Mathematically, similarity distance between data is calculated by Euclidean distance [23]. Figure 13.12 explains the traditional clustering method applied to a data set [24].

5.2.3 Reinforcement Learning

With potential robotic systems in particular, reinforcement learning is recognized as a primary learning method. Within that learning model, it is the duty of the

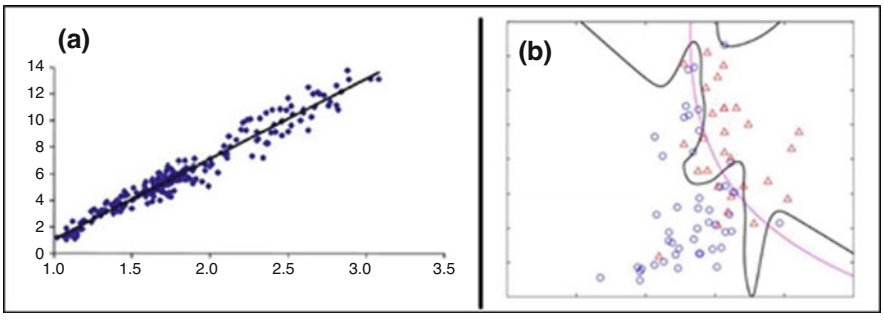

Fig. 13.11 (**a**) Linear regression. (**b**) Nonlinear classification with supervised learning [21, 22]

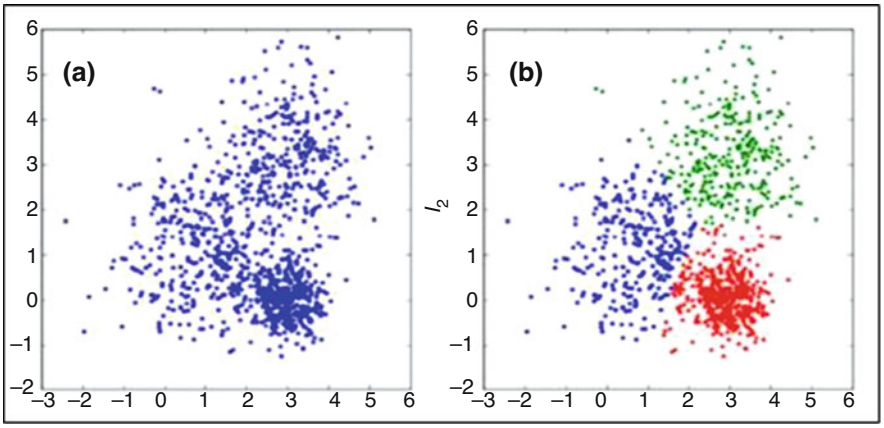

Fig. 13.12 (**a**) Row data scattered. (**b**) Cluster data using an unsupervised learning [21]

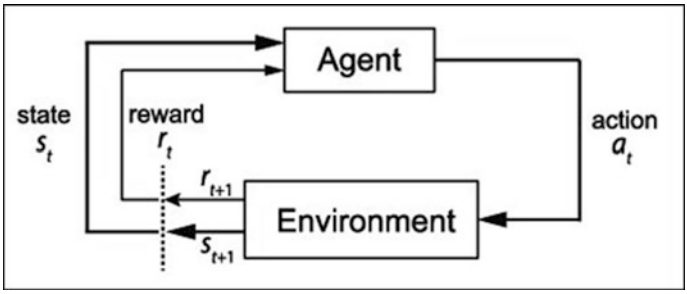

Fig. 13.13 General flow of reinforcement learning [25]

machine learning model to adjust some of its feature space against the effects of its behavior according to the feedback provided. Mathematically, this learning process includes estimating incentive values for such goal acts preparing for future considerations a scheme or data model of behavior. Figure 13.13 reflects a basic flow of reinforcement learning [25].

6 Understanding the Threat Landscape

Adversarial machine learning means designing ML algorithms that can withstand these sophisticated attacks and studying the attackers' limitations and capabilities.

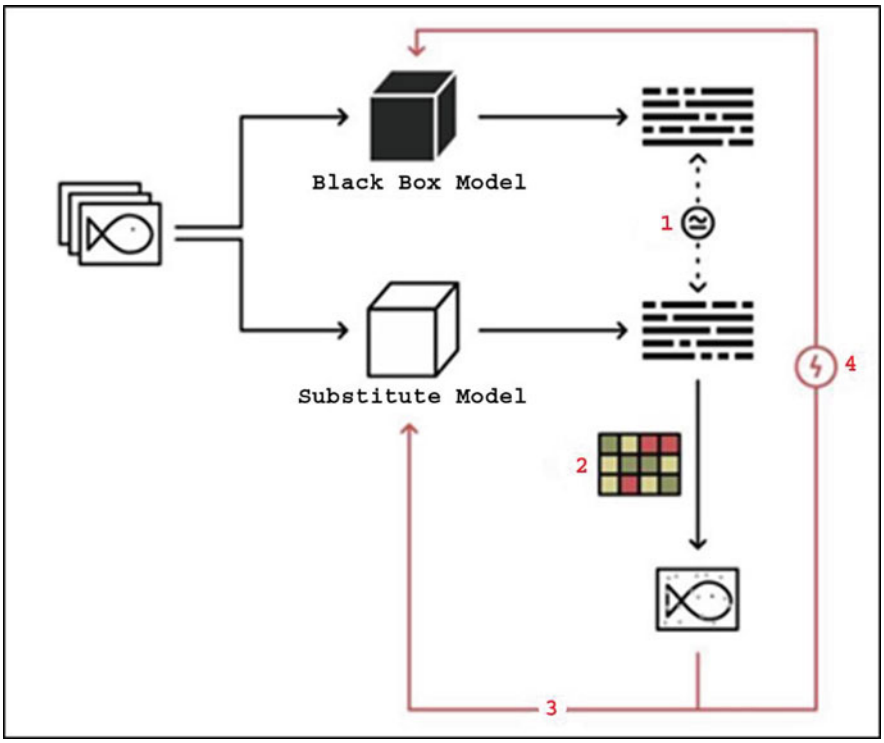

Fig. 13.14 Flow of the substitute attack [27]

6.1 Case Study: Anomalous Traffic Detection

Adversaries may use substitution attacks to interrupt regular user behavior and also to escape by causing the monitor to have a lot of false negatives via an integrity attack. Through doing so, these opponents will limit the risk of detecting their unauthorized activities. When the target machine learning framework is known, some data sets for the artificial training can be generated to allow for decision-making boundaries. As Papernot et al. tested, this technique of black-boxing is considered a substitute attack [26]. Figure 13.14 displays a clear flow of the substitute attack [27].

6.2 Real-World Attacks

Current study said that adversaries feed perturbed data to known models. In addition, the impact of the attacks is assessed using image feature data sets.

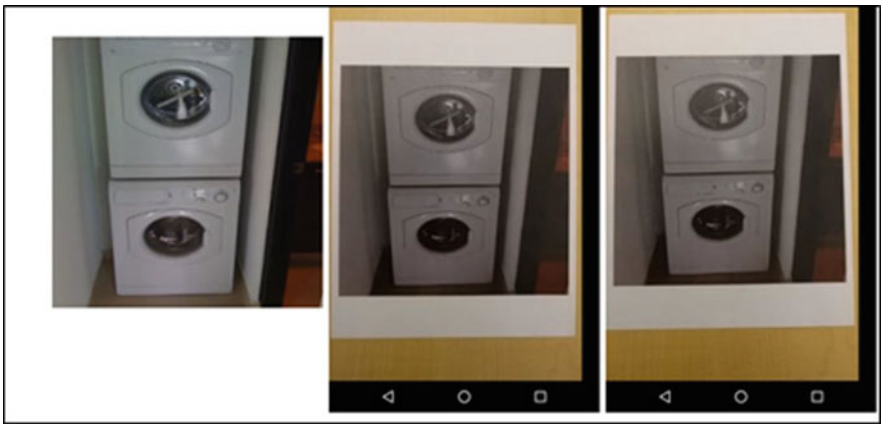

Fig. 13.15 (**a**) Data set image. (**b**) Clean image. (**c**) Adversarial image

Although those environments have proved yourself to be enough to persuade many investigators, this adversarial attack is a major concern for AI. In fact, we find this also from the literature [28, 29], situations where this issue is downplayed and where adversarial instances include real-time issues.

6.2.1 Attack on Cell Phone Camera

A. Kurakin, I. Goodfellow et al. [30] initially revealed that there are risks of threats and attacks even in the physical world as well. They identified adversarial photographs to demonstrate this and took screenshots from a cell phone picture. It has been shown that even when viewed through the camera, a significant fraction of images is misclassified. As Fig. 13.15 explains, the attack on camera pictures is seen here.

6.2.2 Attack on Road Sign

Building on the attacks proposed in [15, 31], Etimov et al. [32] modeled robust perturbations for the physical universe. We also showed the probability of effective attacks on physical environments, such as difference in angles of view, range, and solving. In this work, two attack groups of visible road sign posters were added: (a) poster, at which the attacker designs a distorted sign poster and positions it over the actual sign poster as shown in Fig. 13.16, and (b) sticker disturbance, where the road sign poster is located. The printing takes place on a ledger, and the ledger is stuck over the real label.

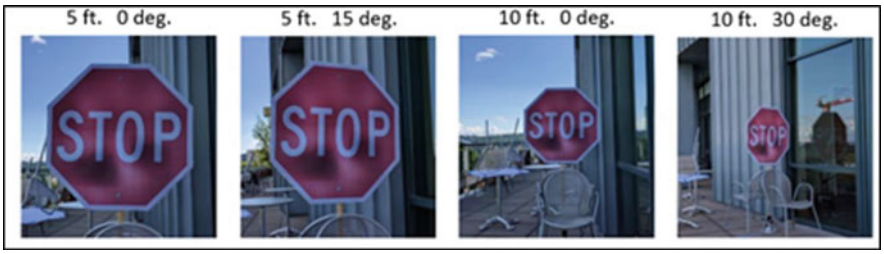

Fig. 13.16 A road sign poster attack [32]: 100 percent fooling LISA-CNN [32] classifier. Even indicating the distance and angle to the image. The classifier is educated for road signs using LISA data set [33]

7 Role of Blockchain for Industrial Automation

Blockchain offers a distributed, immutable, and trusted environment for data storage and transaction processing by using cryptographic concepts to sign, validate, and verify each transaction by miners. Blockchain provides the platform to smart contracts to get executed automatically using consensus algorithms. Currently, many researchers are combining blockchain in various fields like machine learning, IoT, cloud computing, big data analytics, etc. in order to secure the system in a decentralized manner.

Smart contracts attract many industries to automate many things and to eliminate third-party verification. Smart contracts build the trust among unknown entities by providing verification and validation of transactions by special entities called miners. Smart contracts with blockchain attract many industries like health insurance, healthcare, finance, governance, fraud detection, supply chain management, logistic management, natural disaster, self-sovereign identity, and real estate in order to automate various processes and improve efficiency of the overall system [34, 35]. Smart contracts are used in health insurance to automate the process of claiming insurance; for digitization of patient records for surgeries, organ transplant, and OPD in healthcare; to provide a trusted, reliable, and transparent environment to automate transactions in an open distributed system; etc. [35]. Figure 13.17 shows us the various use cases of blockchain where smart contracts can be used for automation, security, and transparency [34, 35] (Fig. 13.18). Table 13.1 shows the various approach that combines 5G, blockchain and IoT for Industrial automation.

7.1 Smart Home

Smart home automation is a prominent technology which aims to change the lifestyle of the people. The application of smartphones provides comfort to the user and also provides security by single access from phone. The architecture of smart

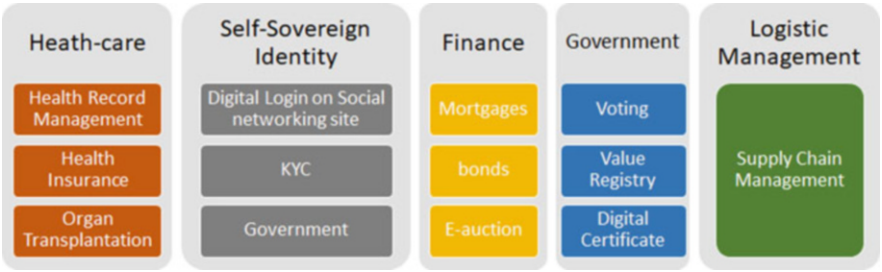

Fig. 13.17 Use cases of blockchain

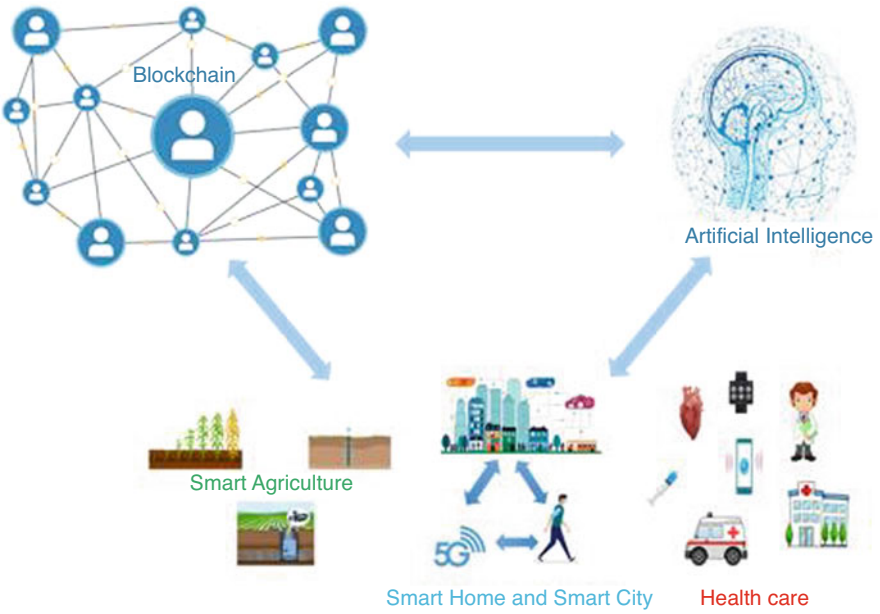

Fig. 13.18 Application of blockchain

homes consists of the network connectivity, sensor, and application. A smart door system plays an important role in the smart home automation. The data is stored in the centralized server so there are chances of the unauthorized person to access the data. To solve this problem, the idea of the blockchain is proposed. Blockchain provides the integrity and authentication to smart door applications. The sensors are used to detect the motion of the person entering into the house through a smart door. Due to blockchain implemented in the smart door, any intruder cannot access the data. Oftentimes IoT devices cannot address the issue; therefore, 5G technology overcomes the limitations.

Table 13.1 Comparison of blockchain approaches for industrial automation

Author	Year	Description	Blockchain technology used	Technique
Jong-ho Noh [37]	2019	Proposed the smart city with blockchain technology. Also listed the issues in the smart city project and solve the security problem using blockchain	Yes	5G and blockchain
Daniel Minoli [38]	2020	The challenges for the smart home with the blockchain for the IoT. The research needs to be done for making use of blockchain in the smart home automation	Yes	IoT and blockchain
Srinivas Jangirala [39]	2019	Limitation in the blockchain-enabled 5G authentication in the supply chain. Proposed an efficient protocol (LBRAPS)	Yes	5G, IoT, and blockchain
Mohamed Amine Ferrag [40]	2020	Proposed the security solution of IoT-based smart agriculture using blockchain	Yes	IoT and blockchain

7.2 Smart City

The migration of the people of villages to the cities increased the number of populations in the urban areas. This leads to the scarcity of the needs to water, food, electricity, etc. To address this problem, smart city projects are implemented which include the use of the IoT and cloud technology. In addition to this, blockchain technology is applied in smart cities. The role of the blockchain is to protect the data of the user from the malicious attack, and blockchain framework allows the entity to communicate in the smart city.

7.3 Supply Chain Management

The activities in the lifestyle of the product involved the organization; resources are the supply chain management. The chain starts from the development of the product to deliver at the user end. The impact of the blockchain and 5G increases the transmission of the product. Blockchain provides the integrity of the product from the development of the product to the end user. The smart contract is the main component of the blockchain which eliminates the use of the third party of having

the decentralized network. Using 5G with blockchain, the tracking of products can be easily done.

7.4 Smart Agriculture

IoT is used nowadays in the agriculture field. Hence smart agriculture comes into the picture, the resultant to improve the product quality and quantity. Sensors can detect the temperature of the soil, water level, moisture, etc. Blockchain is used in the field of agriculture, and the main focus is on the food supply chain. The food supply is connected to agriculture as the raw materials from farmers are taken and used as a product in supply chain management.

7.5 Smart Healthcare

Healthcare is the most essential part in the entire world. With the rise in the population in the world, healthcare conditions are a crucial matter for the government. 5G-enabled IoT is the considered solution in the healthcare domain [36]. The remote system with sensor monitoring system of the patient is useful in healthcare.

7.6 AI and Machine Learning

AI and machine learning algorithms work on the data to train, learn, and make decisions, but data must be secured during the transaction, training, and testing. AI and machine learning work on the set of parameters which must be secured from the unauthorized changes; otherwise, it leads to adversarial effect. Many AI models work on some sensitive information like patient's health data, biometric data for authentication, etc. which must be secured from the intruders as well as to train and deploy the model built on these data using some statistical parameters that need to be secured to prevent adversarial effects. The intruder may manipulate the statistical parameters/environment variables, the devices from where data need to be collected, or the input samples. The attack can be performed on input samples by inserting noise by silently moving the decision boundaries during the training process [41].

Many AI-driven applications like recommendation systems, object detection systems, medical diagnosis, robotic surgeries, etc. use large scale of data which needs to be stored either at some central server or at some distributed environment. Storing data at the central server decreases the chances of external attacks on data and statistical parameters but has the risk of a single point of failure which redirects to adopt a distributed environment. Distributed environment offers many benefits in terms of efficiency, data sharing, and fault tolerance, but due to the involvement of

multiple unknown parties, it leads to trust and security issues. Blockchain solves this problem by providing a tamper-proof distributed environment to build trust among unknown peers without including third-party authority.

In [42], the authors have proposed collaborative training which works in a distributed environment to detect the adversarial attack on any statistical attributes or input samples for convolutional neural network (CNN). This model provides security at network-level attack. The cryptographic concepts and decentralizing properties of blockchain are employed to the CNN model to provide security and accountability. By implementing a hash chain of blocks of CNN models and by hiding the parameters and network scenario, the prevention of threat to any white-box attack is possible. Due to the implementation of hash chain, tempering in any block effect the hash of the current and subsequent block can be easily detected.

In [41], the authors have proposed the secure and decentralized blockchain-based framework for explainable AI (XAI) which is the new and trending field of AI nowadays. This approach provides facilities to record and govern interactions and also allows consensus for predictions and their explanation through the smart contracts to provide security against some adversarial attacks. Blockchain in this framework offers decentralized, reliable, secure, and immutable storage which is built on the top of decentralized applications (DApps). Blockchain can provide transparency and visibility, immutability, traceability, and nonrepudiation using the smart contracts for an explainable AI system.

In [43], the authors proposed the blockchain-based solution for biometrics recognition systems. They covered the traditional architecture of biometrics recognition systems; vulnerabilities at every level of architecture such as feature extraction, template matcher, etc.; and possible solutions for the same. The proposed solution gives alert when alteration occurs at any component of the system. The time complexity of the proposed solution is higher due to complex cryptographic techniques being included to improve the security level.

The integration of blockchain technology with AI models improves security, efficiency, and auditability. It also improves trust among peers for decision-making and fault tolerance. AI enumerates intelligence into the machines over the decentralized blockchain network (Table 13.2).

7.7 Case Study

With the demand of Internet-enabled devices, IoT is also in demand to offer flexible and easy lifestyle to the customers nowadays in the field of healthcare, grids, cities, agriculture, etc. Increasing demand of IoT also increases the requirement of automatic decision-making and intelligent machine to make accurate and efficient decision-making by processing the data collected through various sensors that can be achieved by ML algorithms. IoT network uses resource-constrained devices with smaller memory and smaller computation power that leads to the usage of cloud-based infrastructure for processing of data on cloud-based environment. Various

Table 13.2 AI/ML techniques used in 5G-enabled IoT with key features and advantages

Types of AI/ML methodology	Key techniques	How it's helpful in adversarial attack	Advantages
Classification algorithms-supervised learning	Linear classifiers Logistic regression Support vector machines Naive Bayes classifier Nearest neighbor Neural networks Decision tree Etc.	Monitoring network parameters such as throughput and network fault logs to detect anomalies	Flexible modeling of algorithms with emerging features Agile and self-evolving nature of frameworks for defense
Clustering algorithm-unsupervised learning	Gaussian mixture model K-means Dimensionality reduction Markov decision model	Categorize risks and loopholes of different kinds in network security	Extremely complex data sets for automatic clustering Real-time data discovery
Reinforcement learning	Q learning Gaming algorithm Robot navigation Deep Q learning.	Model learns from the environment Adaptive in nature No training and testing threshold	Highly robust Agent learns from action taken and reward received

machine learning techniques can be used to train the data collected by various sensors to offer intelligence to machines for automatic decision-making. In the area of healthcare, supply chain management, cities, agriculture, etc., many latency-sensitive applications ask for higher bandwidth which can be achieved by 5G network. As seen in the above sections, machine leaning models which use the same set of parameters for training and testing are vulnerable to adversarial attacks which can be attempted by changing the parameter values. Moreover, privacy and lack of control are the major issues in the cloud-based environment. Blockchain is the promising solution which offers security in terms of integrity and transparency. Figure 13.19 shows us the scenario of integration of blockchain with 5G-enabled IoT system which uses cloud infrastructure for processing and storing data.

Here the scenario of embassy which approves the visa of various countries after health examination of the person is taken to show the role of blockchain in integration of 5G-enabled IoT with machine learning through cloud environment.

In traditional visa approval process, medical examination plays an important role. The embassy-certified doctor can examine the person by reviewing immunization and medical history of the person. The patient needs to go through various medical tests like tuberculosis test, urine and blood test, etc. for the fulfillment requirement to get visa of various countries. Nowadays, IoT-based smart healthcare devices can

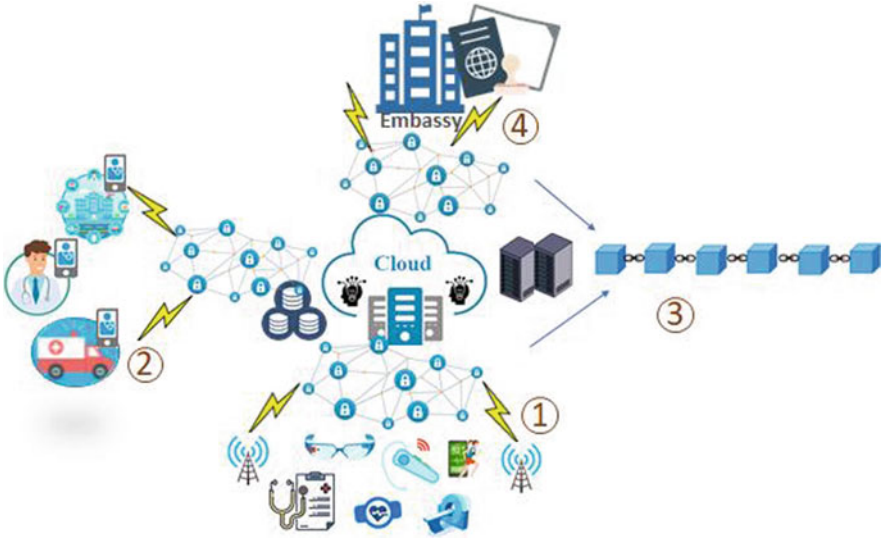

Fig. 13.19 Blockchain-based smart heath examination system for visa approval

examine the person and send the data to cloud for processing. The cloud-based system can share the data received from sensors with doctors and embassy officers for reviewing and visa approval. However, the process of data sharing through cloud saves time and money; the adversarial attack can be easily applied due to lack of control in cloud.

The whole system can be moved on blockchain-based environment with 5G as a communication protocol to achieve integrity, transparency, and higher bandwidth. The scenario is depicted in Fig. 13.19.

8 Challenges of Integrating Adversarial Artificial Intelligence Techniques to Secure 5G-Enabled IoT

The new advances in 5G networks promote the immersive growth of data connectivity through higher data speeds. Such a big rise in data traffic and connected devices suggests further bugs, risks, and attacks that result in financially devastating harm. Artificial intelligence (AI) and machine learning (ML) are intended to play a key role in solving difficult problems of optimization in this context. There is a list of challenges to integrate it with 5G-enabled IoT such as:

- High Bandwidth Demand – The vulnerability and privacy environment from personal devices to the service provider network has also been broadened by increased bandwidth, higher spectrum usage, and fast data speeds in 5G networks. The network should also be clever enough to solve these issues in real time; AI/ML approaches should help model these robust complex algorithms that can help recognize network problems and offer real-time solutions to them which is still challenging.
- Higher-Level Network Heterogeneity – Smart cars, smart houses, smart buildings, and smart cities are supported by 5G-enabled IoT networks. It would require more stable and flexible strategies to deal with essential security problems on both the network and system sides. Intrusion detection using AI/ML by classifying the unauthenticated links would be useful to offer security solution. 5G IoT security and safety can span all levels, such as defense of identity, safety, and machine-to-machine communication. In key authentication, AI techniques found an essential role along with effectively mitigating masquerading attacks.
- Affordable Infrastructure and Lower Cost of Computing – AI/ML consume huge amount of data and train itself. It takes a significant amount of time to process the data collected from IoT devices and store into the cloud. Still optimization is the biggest challenging in the existing algorithm to improve the performance in real time.

9 Conclusion

In this chapter, artificial intelligence has a significant role in automation. Industry 4.0 is the current requirement to develop smart solutions securely. IoT-enabled devices collect huge data and store it over the server. Every transaction between the user to machine and machine to machine can be secured by blockchain technology in terms of integrity. Adversarial machine learning is recent research issues to identify the vulnerability in model and noisy data. Machine learning paradigms provide different learning mechanisms depending on the type of data, continuous data, categorical data, or image data. Types of attack on deep learning algorithms and machine learning algorithms are open issues in computation study. A case study covered in this chapter will be helpful to understand the real-time attack on traffic direction and road signal identification. Some of the researchers have proven the impact of attack in Industry 4.0. To make it 5G-based, IoT-enabled blockchain-based system can be adopted to bypass the various types of attacks on the system. For the enhancement in study, a small survey can be carried out by readers to aware industry to check if their automation systems are preventing attacks and safe for data alteration.

References

1. R.R. Reddy, C. Mamatha, R.G. Reddy, A review on machine learning trends, application and challenges in internet of things, in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, (IEEE, Piscataway, 2018)
2. S. Tanwar, S. Tyagi, N. Kumar, *Multimedia Big Data Computing for IoT Applications: Concepts, Paradigms and Solutions, Intelligent Systems Reference Library* (Springer Nature, Singapore, 2019), pp. 1–425
3. K. Thakkar, R. Thakor, P.K. Singh, M-tesla-based security assessment in wireless sensor network, International Conference on Computational Intelligence and Data Science (ICCIDS 2018), NorthCap University, Gururgram, 07–08th April, Procedia, Computer Science, Elsevier, 1154–1162 (2018)
4. S. Tanwar, J. Vora, S. Kaneriya, S. Tyagi, Fog based enhanced safety management system for miners, in *3rd International Conference on Advances in Computing, Communication & Automation, (ICACCA-2017)*, (Tula Institute, Dehradhun, 2017), pp. 1–6
5. I. Bhudiraja, S. Tyagi, S. Tanwar, N. Kumar, et al., Tactile internet for smart communities in 5G: An Insight for NOMA-based Solutions. IEEE Trans. Ind. Inf. **15**(5), 3104–3112 (2019)
6. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. bitcoin.org (2008)
7. S. Li, L.D. Xu, S. Zhao, 5G internet of things: A survey. J. Ind. Inf. Integr. **10**, 1–9 (2018)
8. M. Agiwal, N. Saxena, A. Roy, Towards connected living: 5G enabled Internet of Things (IoT). IETE Tech. Rev. **36**(2), 190–202 (2019)
9. I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Sig. Process. **135**, 106382 (2020)
10. C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus, Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199 (2013)
11. A. Krizhevsky, I. Sutskever, G.E. Hinton, Imagenet classification with deep convolutional neural networks, in *Advances in Neural Information Processing Systems*, (Morgan Kaufmann Publishers, San Mateo, 2012)
12. I.J. Goodfellow, J. Shlens, C. Szegedy, Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572 (2014)
13. K. Tsui, Perhaps the simplest introduction of adversarial examples ever, Medium.com, 21 Aug 2018 [Online]. Available: https://towardsdatascience.com/perhaps-the-simplest-introduction-of-adversarial-examples-ever-c0839a759b8d. [Accessed 2020]
14. J. Su, D.V. Vargas, K. Sakurai, One pixel attack for fooling deep neural networks. IEEE Trans. Evol. Comput. **23**(5), 828–841 (2019)
15. N. Carlini, D. Wagner, Towards evaluating the robustness of neural networks, in *2017 IEEE Symposium on Security and Privacy (SP)*, (IEEE Computer Society, Los Alamitos, 2017)
16. N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami, Distillation as a defense to adversarial perturbations against deep neural networks, in *2016 IEEE Symposium on Security and Privacy (SP)*, (IEEE, Piscataway, 2016)
17. M. Dezfooli, S. Mohsen, A. Fawzi, P. Frossard, Deepfool: a simple and accurate method to fool deep neural networks, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, (IEEE, Piscataway, 2016)
18. N. Cristianini, J. Shawe-Taylor, *An Introduction to Support Vector Machines* (Cambridge University Press, Cambridge, 2000)
19. S. Lawrence, C.L. Giles, Overfitting and neural networks: Conjugate gradient and backpropagation, in *Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium*, (IEEE Service Center, Piscataway, 2000)
20. U. Kose, Techniques for adversarial examples threatening the safety of artificial intelligence based systems. arXiv preprint arXiv:1910.06907 (2019)

21. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Machine learning models for secure data analytics: A taxonomy and threat model. Comput. Commun. **153**, 406–440 (2020)
22. S. Yang, S. Cai, F. Zheng, Y. Wu, K. Liu, M. Wu, Q. Zou, J. Chen, Representation of fluctuation features in pathological knee joint vibroarthrographic signals using kernel density modeling method. Med. Eng. Phys. **36**(10), 1305–1311 (2014)
23. S.K. Halgamuge, L. Wang, *Classification and Clustering for Knowledge Discovery*, vol 4 (Springer Science, Cham, 2005)
24. A. Gattal, F. Abbas, M.R. Laouar, Automatic parameter tuning of K-means algorithm for document binarization, in *Proceedings of the 7th International Conference on Software Engineering and New Technologies*, (ACM, New York, 2018)
25. R.S. Sutton, A.G. Barto, *Introduction to Reinforcement Learning*, vol 135 (MIT press, Cambridge, 1998)
26. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Tactile internet and its applications in 5G Era: A comprehensive review. Int J Commun Syst **32**(14), 1–49 (2019)
27. R.R. Wiyatno, Tricking a machine into thinking you're milla jovovich and other types of adversarial attacks in machine learning, Medium, 9 August 2018 [Online]. Available: https://medium.com/element-ai-research-lab/tricking-a-machine-into-thinking-youre-milla-jovovich-b19bf322d55c. [Accessed 2020].
28. J. Lu, H. Sibai, E. Fabry D. Forsyth, No need to worry about adversarial examples in object detection in autonomous vehicles. arXiv preprint arXiv:1707.03501 (2017)
29. A.A.R. Graese, T.E. Boult, Assessing threat of adversarial examples on deep neural networks, in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, (IEEE, Piscataway, 2016)
30. A. Kurakin, I. Goodfellow, S. Bengio, Adversarial examples in the physical world. arXiv preprint arXiv:1607.02533 (2016)
31. Y. Liu, X. Chen, C. Liu, D. Song, Delving into transferable adversarial examples and black-box attacks. arXiv preprint arXiv:1611.02770 (2016)
32. K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, Robust physical-world attacks on deep learning visual classification, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, (IEEE Service Center, Piscataway, 2018)
33. J.A. Alzubi, B. Bharathikannan, R. Manikandan, A. Khanna, C. Thaventhiran, Boosted neural network ensemble classification for lung cancer disease diagnosis. Appl. Soft Comput. **80**, 579–591 (2019)
34. B.K. Mohanta, S.S. Panda, D. Jena, An overview of smart contract and use cases in Blockchain technology, in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, (IEEE, Piscataway, 2018)
35. S.R. Mani Sekhar, G.M. Siddesh, S. Kalra, S. Anand, A study of use cases for smart contracts using Blockchain technology. Int. J. Inf. Syst. Soc. Change **10**(2), 15–34 (2019)
36. K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, N. Kumar, A taxonomy of AI techniques for 6G communication networks. Comput. Commun. **161**, 279–303 (2020)
37. J.-H. Noh, H.-Y. Kwon, A study on smart city security policy based on Blockchain in 5G age, in *2019 International Conference on Platform Technology and Service (PlatCon)*, (IEEE, Piscataway, 2019)
38. D. Minoli, Positioning of Blockchain mechanisms in IoT-powered smart home systems: A gateway-based approach. Internet Things **10**, 100147 (2020)
39. S. Jangirala, A.K. Das, A.V. Vasilakos, Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Trans. Ind. Inf. **16**(11), 7081–7093 (2020)
40. M.A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. IEEE Access **8**, 32031–32053 (2020)
41. M. Nassar, K. Salah, M.H. Rehman, D. Svetinovic, Blockchain for explainable and trustworthy artificial intelligence. Wiley Interdiscip. Rev.: Data Min. Knowl. Discovery **10**(1), 1340 (2020)

42. A. Goel, A. Agarwal, M. Vatsa, R. Singh, N. Ratha, DeepRing: Protecting deep neural network with blockchain, in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, (IEEE, Piscataway, 2019)
43. A. Goel, A. Agarwal, M. Vatsa, R. Singh, N. Ratha, Securing CNN model and biometric template using Blockchain, in *IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, (IEEE, Piscataway, 2019)