**A comprehensive Analysis of Various Threat Detection and Prevention Techniques in IoT Environment**

[1]Pavithra P S, [2]Dr.P.Durgadevi,

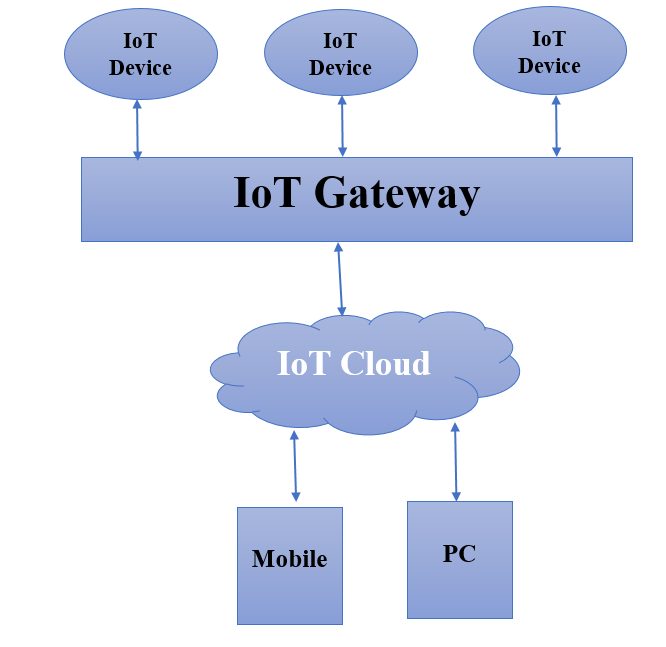
[1] SRM Institute of Science and Technology, [2] SRM Institute of Science and Technology [1] pp2616@srmist.edu.in, [2] [durgadep@srmist.edu.in](mailto:durgadep@srmist.edu.in)

# ABSTRACT

The Internet of Things (IoT) has become one of the most widely used technologies in the recent times. IoT device can be enabled to collect, and exchange information in a highly efficient manner via the network. A Smart object with technology and devices build a network infrastructure that is used in a variety of areas such as mechanical, building, medical, manufacturing, entertainment, and transport. The Major security issues such as confidentiality, authentication, confirmation, security systems, system configuration, data storage, and administration are the main challenges in an IoT environment. To overcome these security issues, various techniques are addressed. Initially an Intrusion Detection System (IDS), is a software that monitors a network of Malicious activity using valuable tools in IoT devices. Then, Machine technique helps to detect the attacks from intrusion detection system to provide embedded intelligence in an IoT devices and networks. Finally, Blockchain (BC) technology is gaining traction in modern IoT devices to address security and privacy challenges to provide reliable communication in an IoT environment. The aim of this work is to provide a detail review of ML and BC techniques that can be used to develop improved security IoT device methods.

# 1.INTRODUCTION

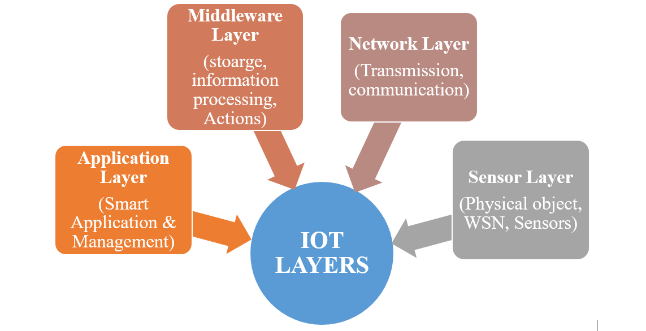
IoT is a connection of sensors and objects that can communicate with one another without human intervention. The "things" in the IoT are hardware objects, such as wearable sensors, that detect and collect different types of data about technology and human social activity. The Internet of Things keeps people, objects, devices, and services all interconnected at all times. The primary objective of the Internet of Things is to create a broadband network with interrelated communication systems and application that helps physical/virtual sensors, home computers (PCs), digital phones, motorcars, and items such as fridges, washing machines, household appliances, food, and medications to be connected and embedded anywhere at time and on any network. The requirements for large-scale IoT deployment are rapidly growing, posing a serious security issue. Privacy, authorization, authentication, security systems, system configuration, data storage, and monitoring are the primary issues in the IoT environment. [1].  IoT devices link to complex devices, interact with dangerous environments, and are deployed on a wide range of unmanaged systems, they confront a number of security concerns and challenges. The Internet of Things layer is separated into four layers; its architecture is based on standard Online communication network, and it is primarily for information transit between IoT devices. In recent years, IDS has shown to be a more reliable and efficient strategy. IDS is technology that analyses a network for unexpected IoT device performance. [3] IDS can be set up on a single system or on multiple machines in a network. IDS provide a number of advantages to businesses, including the ability to detect security threats. An IDS (figure 1) can aid in the identification of threat types and numbers. This paper outlines a strategy for developing an IDS that employs Machine Learning (ML) approaches to detect data-based threats in order to defend against attacks in the IoT. The hostile devices carry out attacks, data is collected in two ways: benign information during normal flow and traffic seized during threats. Machine learning techniques built using a number of approaches to detect malicious behaviour in an IoT infrastructure. Blockchain is a distributed technology with numerous advantages, including increased security and transparency. As a result, blockchain has the potential to be a strong platform for payment and communication apps. IoT services and applications are, by design, dispersed. This means that by using blockchain as a database to keep records of how things communicate, what state they're in, and how they connect with other IoT systems, blockchain can help to solve the majority of IoT privacy and tracing issues.



**Figure1** IoT Architecture

The detail review of this paper carried as follows section 2 classification of IoT layers and its protocols section 3 security issues in IoT Layers section 4 security issues using IDS, Section 5 security issues using ML Techniques and section 6 security issues using Blockchain technology

# 2. CLASSIFICATION OF IOT LAYERS

The IoT can be divided into four layers namely Application, Middleware and sensor Layer, as shown in (Figure 2)

**Figure 2** IoT Layers

**2.1 APPLICATION LAYER**

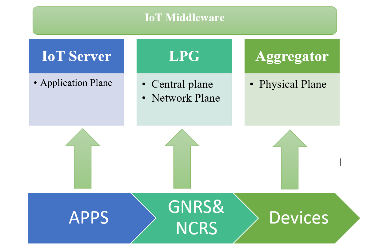
The advantages of IoT in our daily lives are obvious. Security was not a design aim when the IoT was first introduced in the late 1960s since security risks were not properly grasped. Security has become critical for the IoT's long-term viability and widespread adoption. IoT applications and sensors have infiltrated every part of our life [2]. IoT has become a critical component of many healthcare contexts. IoT sensors have made their way into our living environments, allowing for home automation and the creation of intelligent, highly homes. Possible source, led lights, thermostats, and other home items are now equipped with networking capabilities, enabling for wireless remote control. Almost every household item can be changed with an autonomous, remote-controllable replacement. We are enveloped by IoT apps and devices in our homes, automobiles, railroads, roads, transport, farming, and companies, as seen in (Figure 3).



**Figure 3** Application Layer

**2.2 MIDDLEWARE LAYER**

Middleware for the IoT devices is technology that acts as an interface between Network elements, improving interaction between elements that would otherwise be incompatible. Middleware combines disparate, often sophisticated, and already-existing programmes that were not linked in the first place. IoT is defined as the ability for almost anything (anything) to be interconnected and transfer data through a system. Middleware (figure 4) is a component of the design that enables connectivity for a large number of different Things by giving a connection layer for the network layer as well as the application layers that provide solutions that enhance efficient software interactions.

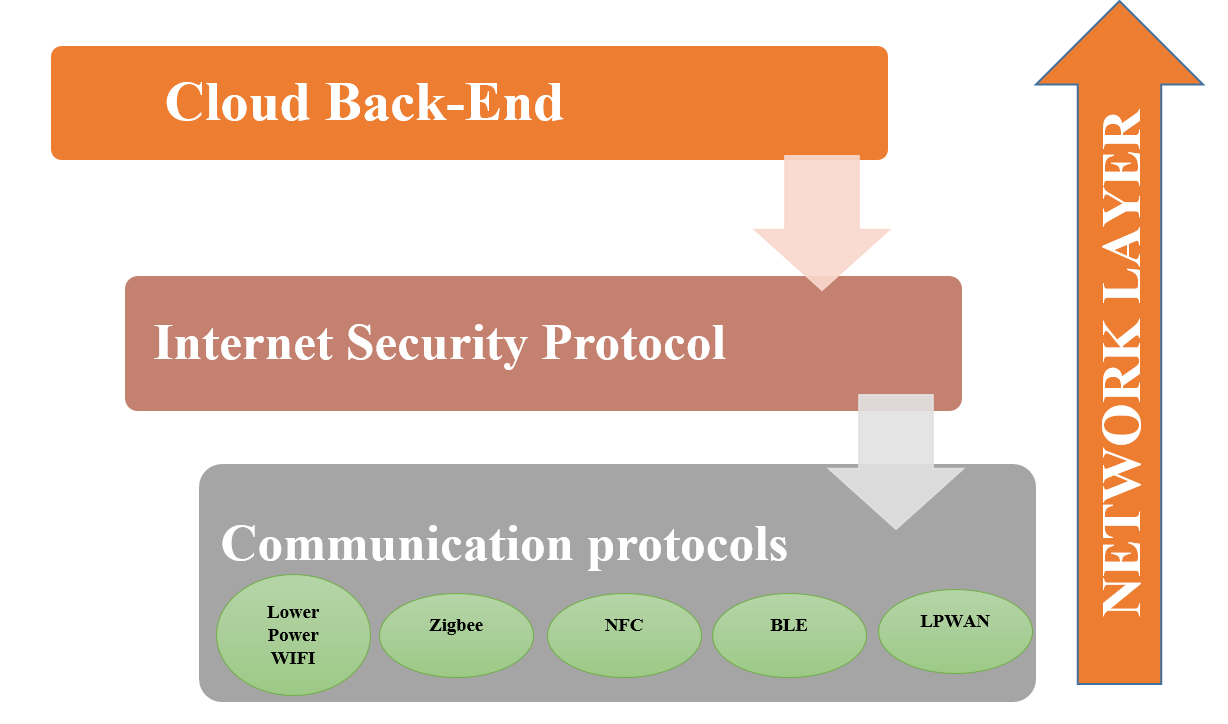


**Figure 4**  middleware Layer Protocols

The Aggregator, Local Service Gateway (LSG), and IoT server are the three basic layers of IoT middleware. Sensor abstraction is provided by the aggregator, which hides the hardware characteristics of the actual sensors and presents a single interface for searching and subscription to sensor data. The LSG layer receives raw data from the aggregator [4]. The LSG connects the Internet of Things system to the rest of the world. For contextual refinement and aggregation purposes, it may analyse basic data given by the aggregator. The LSG also sends the data to the IoT server, along with a data GUID, user access framework, and memory location information (human-readable names or NA). Through its edge router, programs (users) can request the IoT server about where to get information from. The data can then be retrieved from a storage place or right from the aggregator. The IoT server can select whether to perform network access internally or outsource it to the NCRS/GNRS. Huang and colleagues offer a security paradigm for the Internet of Things that aims to find the balance between security and usability. A body-area networking, a home network, and a motel network are three key scenarios where customer experience is vital. A logistics IoT scenario and an office IoT situation were also studied. A survey has been done to fully understand consumer perceptions of the relevance of safety vs. accessibility, as well as how ready users are to sacrifice one for the other. Authentication, consistency, and accessibility were three characteristics of security that users were asked about. While different components of safety matter vary depending on the specific application, the survey results reveal that security is important to all people and in all apps. This is especially true when it comes to security and payment services.

**2.3 NETWORK LAYER**

The network layer controls data transfer to and from various products or applications using a range of assessment methods and techniques across wired or wireless communications. The network layer takes the analyzed data from the perception layer and calculates the optimal methods for transmitting it via form products to IoT devices, ports, and bridges. (figure 5)



**Figure 5**  Network Layer protocols

##### **2.3.1 Low Power WiFi**

Devices that enable WiFi, like some other Wireless connections, IP communication is also supported by HaLow, which is vital for Iot systems. Let's take a look at the IEEE 802.11ah standard's characteristics. This standard was created to deal with resource sensor network applications that demand particularly long communication. IEEE 802.11ah runs at 900 MHz in the semi range [5]. The range is greater due to lower frequency, while greater range waves suffer from greater absorption. We can increase the range (now 1 kilometre) by lowering the frequency, but the data rate will be reduced as well, thus the compromise is not justifiable. Huge star-shaped networks, where many nodes are connected to a specific access point, are also supported by IEEE 802.11ah.

**2.3.2 Zigbee**

It is used for local area networks, or PANs, and is based on the IEEE 802.15.4 communication protocol standard. The Zigbee partnership, which aims to develop dependable, low-energy, and low-cost communication technologies, created Zigbee. The communication range of Zigbee devices is fairly short (10–100 metres). The Zigbee standard also specifies the details of the network and application levels. The network layer here, unlike BLE, allows for multichip routing.

**2.3.3 Near Field Communication (NFC)**

NFC is a very Small-range wireless transmission technology that enables portable devices to communicate with each other across a few millimetres [6]. By bringing two NFC-enabled devices close to one other, any form of data can be exchanged in seconds. RFID is the foundation of this technology. It communicates information between multiple NFC-enabled devices by utilising magnetic field fluctuations. NFC uses the 13.56 MHz frequency range, which is the same as high-frequency RFID. Active and passive modes of functioning are available. Both devices produce magnetic fields in active mode, however in passive mode, only one device produces the field and the other transfers data through load modification. In rechargeable batteries devices, the passive mode is useful for maximising energy efficiency. The requirements of close proximity between devices has the advantage of facilitating data security such as payments. Finally, unlike RFID, NFC can be utilised for bidirectional communication. As a result, practically every smartphone on the market today supports NFC.

**2.3.4 BLE**

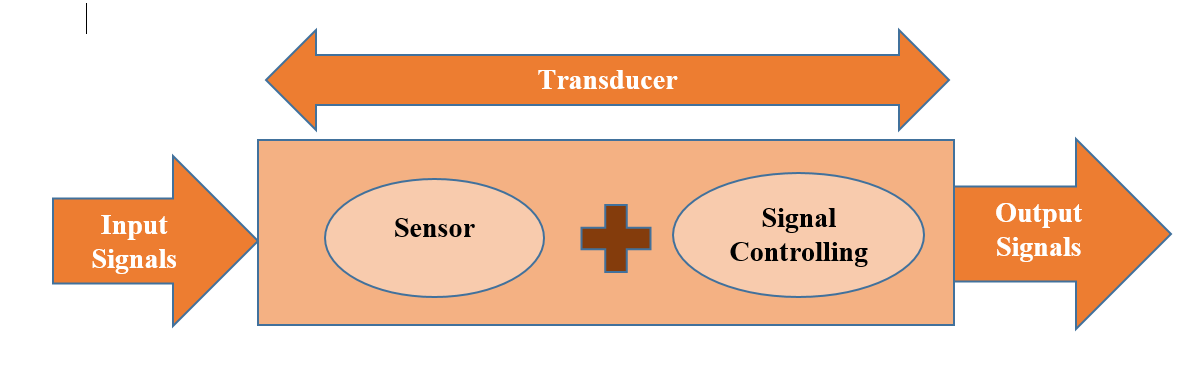
The Bluetooth Special Interest Group formed Bluetooth Low Energy, popularly called as "Bluetooth Smart." When compared to rival procedures, it has a shorter range and uses less energy. The BLE communication devices is comparable to that used in traditional Bluetooth. It consists of two parts: the actuator and the client. The hardware and connectivity layers are implemented by the device. The computer is often a SOC with a Tv. The uppermost layers' capacities are contained in the server. BLE is inconsistent with traditional Bluetooth. Consider the differences between standard Wifi and Bluetooth Low Energy (BLE).

**2.3.5 Low Power Wide-Area-Networks (LPWAN)**

The low-power wide area network (LPWAN) is a communication network for connecting reduced, rechargeable batteries objects over long distances [7]. LPWANs, that were built for M2M and internet of things (IoT) networks, are less expensive and consume less power than traditional wireless services. They can also connect a greater variety of mobile over a greater distance. LPWANs can accept data traffic varies from 10 to 1,000 bytes at upload rates of up to 200 Kbps. The distance of an LPWAN can range from two km to 1,000 km, depending on the method. Most LPWANs have a network system, similarly to Wi-Fi, in which each destination communicates to a central hub.

**2.4 SENSOR LAYER**

For all IoT systems to gather information from the environment, one or more sensors are necessary. Sensors are a crucial component of intelligent devices. Environment information is one of the most crucial parts of the Internet of Things, which is impossible to achieve without sensing devices. Sensors for the Internet of Things are usually compact, low-cost, and source of energy (figure 6). They are limited by variables like storage capacity and easy installation. To give a broad overview of the different types of detectors that can be used to develop effective solutions



**Figure 6** sensor Layer

**2.4.1 Mobile Phone Sensors**

First, consider the omnipresent mobile phone, which contains a variety of sensors. The smartphone, in particular, is a particularly convenient and user-friendly device with a variety of built-in connectivity and information processing features. Because of the integrated sensors, researchers are expressing interest in developing smart IoT solutions employing mobile phones as a result of their growing popularity. Depending on the situation, extra sensors may be required. On the smartphone, software can be created that leverage sensor data to provide useful outcomes. The following are some of the sensors found inside a smart device [8]. A smartphone phone's sensor detects motion and acceleration. It usually measures changes in the smartphone's movement in three dimensions. Accelerometers come in a variety of shapes and sizes. An earthquake mass in a housing is linked to the building using a springs in a physical accelerometer. Because the mass moves slowly and is left behind when the housing moves, the force in the spring can be linked to the acceleration.

**2.4.2 Healthcare Sensors**

IoT can be tremendously benefits in health applications. Devices can be used to evaluate and monitor a wide variety of clinical works in the body. The apps can be used to monitor a patient's condition while they weren't in the healthcare setting alone. The physician, relatives, or the patients can then receive real-time feedback. McGrath and Swanbill have gone into great length about the sensing devices that can be carried on the physique to track a people's ability.

**2.4.3 Neural Sensors**

It is now possible to read brain waves, estimate the brain's condition, and educate the mind to enhance focus and attention. This is known as neurofeedback. The technique used it to detect mind waves is EEG or a brain parts connection. Physical interactions between nerve cells produce electric field that can be defined in terms of wavelengths externally. Brain are categorised Delta, theta, gamma, Beta, and alpha waves based on frequency.

##### **2.4.4 Environmental and Chemical Sensors**

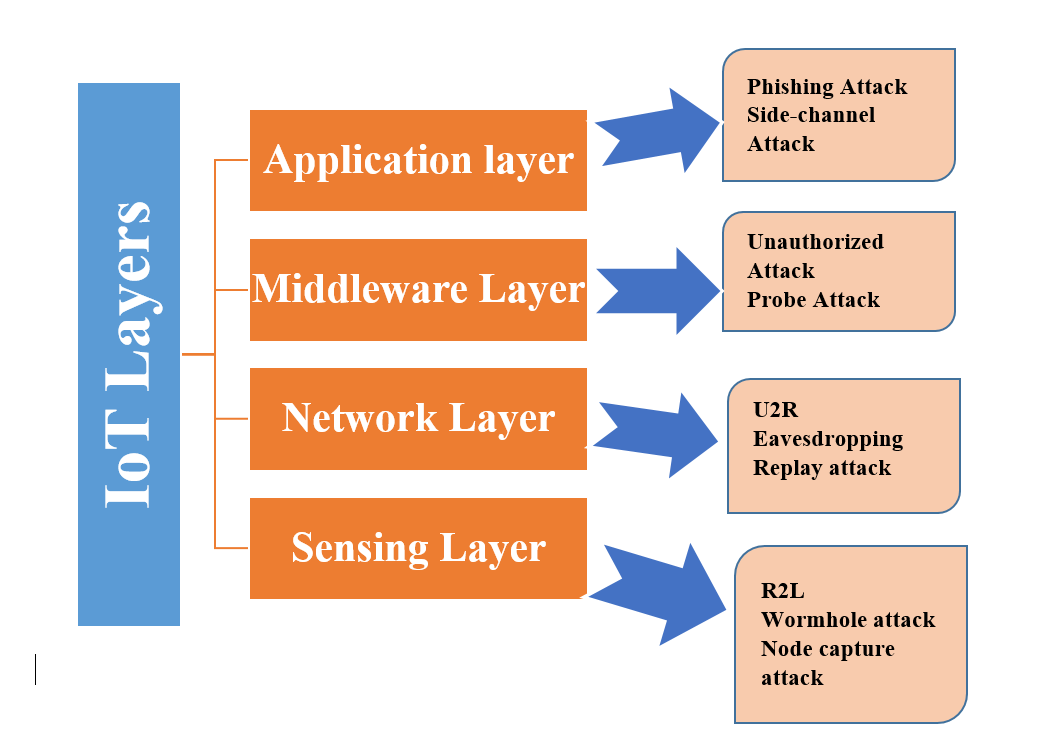
##### ES detect physical elements in the physical surroundings such as temperatures, moisture, force, water contamination, and air quality. Temperature and humidity can be measured with a thermostat or a gauge. Air quality can be determined using sensors to monitor the existence of chemicals and other particulates in the atmosphere. Chemical sensors can detect biological and chemical substances. These sensors are made comprised of a reference electrode and an actuator. Individually, the electroscope (e-nose) and electronics tongue (e-tongue) are devices for detecting chemicals based on aroma and taste. The e-nose and e-tongue are made up of a variety of sensing devices and powerful pattern recognition software. The e-nose and e-tongue sensors produce complex data, which is evaluated using predictive modelling to identify the input.

##### **2.4.5 RFID**

RFID (radio frequency identification) is a type of proof of identity in which information is conveyed by an RFID tag (a small chip with an antenna) and received by a RFID reader. Radio waves are used to send the information stored on the tag. It functions similarly to bar code technologies. It's doesn't, though, need line-of-sight connection between both the tracker and the sensor, and it may recognize itself without the help of a single operator at a distance. RFID range is determined by frequency. It can grow to be hundreds of metres long.

**3. VARIOUS SECURITY ISSUES IN IOT LAYERS**

The Internet of Things encompasses a wide range of devices and technology, from small embedded devices to advanced massive servers. There is a need to draw attention to security concerns at various IoT tiers. A taxonomy of IoT security challenges, as well as security solutions for each tier of the IoT. The four layers of the most popular IoT layer architecture are sensor, network, middleware, and application. These four layers contain a wide range of data (figure 7), as well as many enabling technologies and features. In addition, the following sections outline the IoT/IIoT levels, as well as the security threats that each tier faces.



**Figure 7** Security Threats in IoT Layers

**3.1 Phishing attacks**

The goal of this attack is to steal user login credentials for any IoT interface. To attract real users, an opponent presents phoney or spoofing links. The adversary takes their login credentials once they supply them to the false portal. Finally, the adversary logs into the private IoT interface using these identities.

**3.2 Side-Channel Attack**

The malevolent adversary seeks for the encryption keys in this assault. Adversaries use electromagnetic analysis and device power usage analysis in this type of Threats.

**3.3 Unauthorized Access**

When it comes to security, IoT networks are notoriously lax. An adversary can simply get access to the IoT network infrastructure by using unsecured ports and back doors. They can conduct a variety of attacks once they have gained access to the network.

**3.4 Remote to Local (User) Attacks (R2L)**

This sort of threat transmits messages over the network in the hopes of attacking security flaws and gaining unwanted remote access to the system. Some of the tools that go after incorrect or poor security measures include Ftp-Write, Xsnoop, Visitor, and the Dictionaries. The Xlock technique is another technique that uses social engineering to get access.

**3.5 Probing**

Probing is a sort of attack where the attacker explores a network for vulnerabilities such as ports and services that can be used to locate services operating on the resource. By attacking a security vulnerability, they often gain privileges to an unwitting host.

**3.6 User to Root Attacks (U2R)**

Buffer overflow is the most common U2R attack. This class starts by getting access to a frequent user and searching for usernames in order to gain root account access to the computer resource.

**3.7 Eavesdropping attack**

This sort of attack monitors the message sent to an RFID reader with authorised by RFID tags to identify the wavelength and tagging groups used by RFID tags. The bulk of RFIDs use plaintext because of price and storage limits, allowing for effective eavesdropping**.**

**3.8 Node Capture Attacks**

In these cyber intrusions, attacker’s collection a node or change devices, generating sensitive information for the implementation of digital rights like connectivity keys. The entire Iot platform becomes unsafe if substitute nodes act illegally.

**3.9 Replay attack**

Following eavesdropping on transmissions send by a system with the appropriate transmitter and chip, and then copying an identification unique number used by an Eligible user, this form of threat includes copying the approved tag or sending a message again. Some information, which is sent via the tag, is required for active attacks.

**3.10Wormhole Attack**

Cyberattacks against traffic patterns and network categorizations are common targets. Wormhole actions are carried out by constructing a tunnel between both intruders that enables information to be freely passed across it.

**4. IOT SECURITY**

As we addressed some of the security challenges in the previous section, we will provide some of the methods for protecting IoT risks in the network. There are three primary ways for securing the IoT environment: 1) Intrusion Detection System 2) Machine Learning Techniques 3) Blockchain technology Below are some in-depth explanations of the approaches described.

**4.1 IoT security using IDS**

An Intrusion Detection System (IDS) scans network traffic (Table 1) for detecting anomalous activities and notifies the user. The fundamental goal of an IDS is to identify suspicious behaviour and notify it to the system administrator; however, certain IDS software takes action based on rules if harmful activity is discovered.

**Table 1** Threat Monitoring Tools using IDS

|  |  |  |  |
| --- | --- | --- | --- |
| **Tools** | **OS Type** | **IDS Types** | **Features** |
| **Snort**  [Snort logo](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/12/Capture-3.jpg) | Unix, Linux, Windows | NIDS | * Security information, network analyzer, network recorder Removing signatures, * Safety fingerprints are updated frequently. * Detailed analysis, * OS identification, Vulnerability scanning, Data corruption, buffer overflow attacks, and hidden penetration testing are all examples of occurrences that can be detected. |
| **Suricata**  [Suricata logo](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/12/Capture-4.jpg) | Linux, Mac Os, Windows, unix | NIDS | * Information is collection at the application network. * Connectivity with 3rd tools like BASE, Squil, BASE, and Anaval, built-in script module, signatures and anomaly-based approaches, and a smart input sequence |
| **Bro-IDS**  [Bro logo](https://www.softwaretestinghelp.com/wp-content/qa/uploads/2019/12/Capture-1.jpg) | Unix, Linux, Mac-OS | NIDS | * Recording and analysis of traffic * Transparency between packages is provided. Policies scripts, events engine * Monitoring SNMP traffic is possible. * FTP, DNS, and HTTP traffic can all be tracked. |
| **Kismet** | Unix, Linux, Windows, Mac-OS | HIDS | * Transparent HIDS security that is easy to use * The possible to identify any changes to the Windows system, * On Mac OS, the ability to monitor any attempts to gain root privileges user, * Mail, FTP, and web host records are all covered. |
| **OpenWIPS** | Windows, Linux | NIDS | * Sensors: "Stupid" sensors that catch wireless signals and relay it to a database for evaluation. * Server: Combines information from all devices, analyses it, and reacts to assaults. * GUI runs the servers and shows threat data on your wireless network (s). |
| **Onion Security** | Linux, Mac-OS | HIDS, NIDS | * A comprehensive Linux installation with an emphasis on data collection and management, business video surveillance, and intrusion detection Works on Linux and contains aspects from Network Miner, Snorby, Xplico, Sguil, ELSA, and Kibana, among other analytic and front-end tools. * Also includes HIDS features, a traffic analyzer for networking investigation, and attractive charts and graphs. |
| **Solar winds** | Windows | NIDS | * Specify the amount and kinds of threats, reduce manual detection, show compliance, and so on. |

**4.2 IoT security using Machine Learning Techniques**

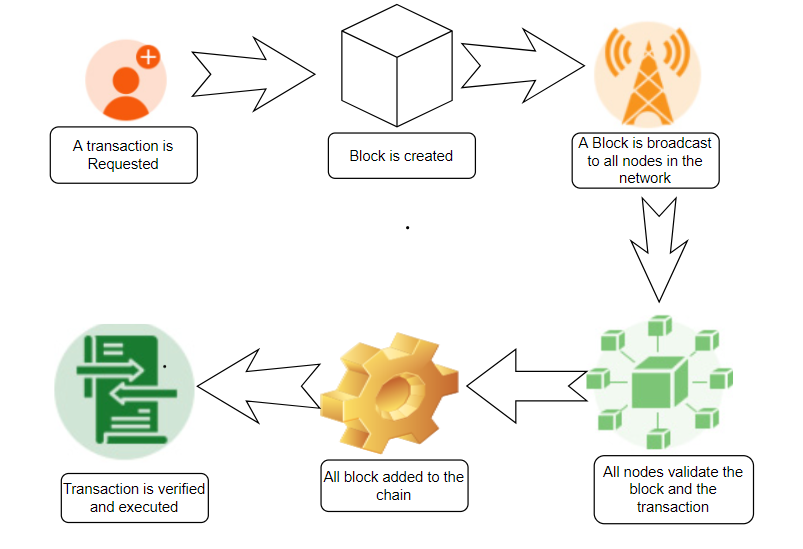
The investigations were categorised using machine learning methods for detecting IoT risks. The table lists the authors of the articles, as well as a summary of their work, datasets, and machine learning techniques employed. Several studies have discussed framework concepts, IDSs, techniques, and smart designs to detect threats and attacks in IoT devices, while Ml algorithms are the most promising for providing security in the IoT context. According to the overview of studies, Support Vector Machine, Decision Tree, Random Forest, NB, KNN, and fuzzy algorithms (Table 2) are frequently used to address information security difficulties. There are three types of learning-based Ml techniques: supervised, unsupervised, and semi-supervised. Moreover, many studies measured the effectiveness of efficient hybrid models, which combine various approaches.

**Table 2** Threats Detection using ML Techniques

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Author** | **Threats** | **Description** | **Tools** | **Dataset** | **ML Algorithm** |
| Erhan, et al [9] | Phishing attacks | Using the BoT-IoT recognition database to determine if ML approach is more effective, a new development methodology and a hybrid technique were provided to address the difficulty of Ml techniques for internet.. | Snort | UNSW-NB 15 | Decision Tree, Random forest |
| Jeon et al [10] | Side-Channel Attack | This research proposes both semi-distributed and decentralised techniques for resource-constrained sensors that support higher feature extraction and selections with possible fog-edge coordinating analysis to overcome the limitations of highly centralized IDS. | Suricata | Bot-IoT dataset | KNN,  SVM |
| Suhail et al [11]. | Unauthorized Access | CEP and Machine Learning (ML) were used to develop a smart method that enables CEP and ML to detect Network communication risks in real time. In particular, such a design is capable of rapidly controlling sequences whose requirements are defined using machine learning approaches. | Bro-IDS | AWID dataset | RF, XGBoost |
| Kshirsagar et al [12]. | Remote to Local Attacks (R2L) | This study evaluates the performance of the false alarms alert decrease categories using both datasets in real network conditions. | Kismet | MQTT regular traffic packets | K-means clustering, Linear Regression |
| Zhang et al [13]. | Probing | For virus identification and classification in IoT, converts the apps' OpCodes into a subspace and applies fuzzy and fast fuzzy patterns graph methods | OpenWIPS | KDD99 | Logistic Model Tree, RF |
| Moustafa et al [14]. | User to Root Attacks (U2R) | Suggests a threat intelligence analysis of energy systems machine learning algorithms that may be developed utilising data and archives collected by phase control monitoring units (PMUs) | Onion Security | NSL-KDD | DT, KNN |
| Abdullah et al [6] | Eavesdropping attack | Multiple machine learning models were used to compare anomaly and threat detection in IoT data. | Solar winds | Bot-IoT | MLP, kernel approximation |
| Bagaa et al [15]. | Node Capture Attacks | The researchers provide an internet backbone, behaviour patterns anomaly detection system for protecting IoT settings, in which the unpredictability of Data transmission from IoT devices can be used to detect different dos attack in real time employing machine learning. | Snort | UNSW-NB15, CICIDS2017 | Auto encoders, MLP |
| Tawalbeh et al [4]. | Replay attack | Suggests the use of the correlation subset obtain (CST-GR) criterion, an unique attribute selection method, to determine suitable capability for a lightweight IDS based on machines that employ a novel control strategy. | Suricata | IoT traffic | SVM, kernel approximation |
| ErhanS et al [9]. | Wormhole Attack | This research looks at an algorithm-based attack and identify suspicious technique for detecting and reducing IoT cybersecurity risks in a smart city. | OpenWIPS | Simulation of IoT device | XGBoost, MLP |

**4.3 IoT security issues using Block chain**

Blockchain networks can be set up in centralised or decentralised configurations, each with its own set of advantages and disadvantages. The early is better for large data transmissions across systems, whereas the latter is superior for versatility and real-time services. Blockchain can help standardise activities across a wide range of devices, as well as improve confidence across unsuitable connections or devices features that interact with each other (figure 8). Proposed blockchain solutions ensure a greater level of security by network architectures trust and worldwide identity, standardized and high-level identification, situational privacy, and exponentially protection against high-level intruders without compromising IoT flexibility.



**Figure 8** Blockchain Process

## **4.3.1 Ethereum**

The Ethereum digital solutions technology is a very well and widely used in the business. In actuality, it is the world's first blockchain development environment. A software system is a purpose and state-based system software. At a specific address, each intelligent contract runs on the Ethereum platform. Smart contracts may send transactions and have balance since they are an autonomous sort of account on Ethereum. The EVM allows you to construct Ethereum-based decentralised programmes (DApps). Etheruem is a permissionless ledger that may be used by anyone. It uses proof of work as its consensus process, which is known to be slow.

**4.3.2 Hyperlegder Fabric**

## The Hyperledger Hub created Hyperledger Fabric, a public blockchain distributed ledger platform. The Linux Fund's Hyperledger Hub is an initiative promoting public research of both centralised and decentralised blockchain technologies. Not only does Blockchains have a public blockchain ledger like Ethereum, but it also has a modular design.

## **4.3.3 Hyperledger Sawtooth**

Hyperledger Sawtooth is another Hyperledger Hub modular blockchain technology for building distributed ledger systems and services. The Linux Foundation launched Hyperledger Sawtooth, which is presently supported by IBM and Digital Assets. Hyperledger Sawtooth is used by businesses to develop scalable and reliable systems and to deploy highly secure blockchain applications

**4.3.4 EOSIO**

Block one launched EOSIO, a high-performance open-source blockchain technology, in 2018. EOSIO is a blockchain application development platform that is quick, dependable, and secure. Smart contracts can be deployed on EOSIO's current networks. You can also create your own EOSIO networks and use them to deploy smart contracts.

**4.3.5 Corda**

## The R3 Consortium created Corda, an open-source blockchain technology, in 2015. Corda was created with financial institutions. "The DLT platform of choice for financial services and beyond," the next-generation blockchain framework claims. Corda supports smart contracts and has a permission ledger type, so you can build and deploy smart contracts on the Corda blockchain. Smart contracts in Corda can be developed in either Java or Kotlin. Because the platform lacks a mining capability, most nodes never see a portion of the transactions. To put it another way, Corda transactions aren't available to all nodes. Corda does not have any cryptocurrencies or tokens.

## **4.3.6 Quorum**

Quorum is an Ethereum-based open-source blockchain platform. It was created in 2016 with the intention of serving the financial industry and allowing businesses to "use Ethereum for their high-value blockchain applications." ConsenSys just purchased Quorum from JP Morgan. Enterprises that wish to use the blockchain technology for their business might get help from Quorum. It features a permissioned ledger type, but it also allows for client-specific customizations. Quorum's smart contracts are designed in Solidity, making the transition from Ethereum to Quorum a breeze.

**4.3.7 Distributed Ledger**

Bitcoin's launch cleared the door for a new and decentralised payment system with a built-in trust mechanism. The Bitcoin system, in particular, does away with the necessity for a centralised institution to handle and verify money transfers. Since the introduction of Bitcoin, a slew of platforms has sprung up to facilitate peer-to-peer transactions in a decentralised setting. To establish a decentralised and reliable platform, Blockchain technology combines cryptography, consensus algorithms, distributed ledgers, and, optionally, decentralised compute power.

**4.3.8 Peer to Peer communication**

Peer device communication is an important part of IoT solutions that should not be disregarded. The Internet of Things [20] is built around it. P2P systems for IoT device exchanges are developed as a result, for IoT device operating as a network node. When combining IoTs with blockchain, the fundamental design decision must be made at which level or phase their peer-to-peer communications will occur, i.e. the blockchain, Effectively from one IoT peer to some other peer, or via a composite design architecture.

**CONCLUSION**

In this Paper, we discussed the various levels of architecture, applications, and protocols used in the IoT environment. In this study security threats that exist at various layers of the IoT network and we covered current and future IoT security solutions such as intrusion detection systems (IDS), machine learning, and blockchain technology. From this discussion we proposed that there is high security risk in network and sensing layer. Using hybrid IDS framework tool, we can monitor the malicious activity continuously in IoT network then using Hybrid machine learning techniques, it helps to detect the unknown attacks with less consumption time and high accuracy and prevent the security issues using efficient blockchain technology.

**REFERENCES**

[1]. Mcginthy, J.M.; Michaels, A.J. Secure Industrial Internet of Things Critical Infrastructure Node Design.IEEE Internet Things J. 2019, 6, 8021–8037.

[2]. Lee, S.K.; Bae, M.; Kim, H. Future of IoT Networks: A Survey. Appl. Sci. 2017, 71, 1072.

[3]. Lee, I.; Bae, M.; Kim, H. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12, 157.

[4]. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. Appl. Sci. 2020, 10, 4102.

[5]. The State of IoT Security. October 2017. Available online: https://www.gemalto.com/m2m/documents/iot- security-report (accessed on 5 September 2020).

[6]. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. In Proceedings of the 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019, Riyadh, Saudi Arabia, 1–3 May 2019; pp.1–6.

[7]. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Wirel. Commun. 2018, 25, 12–18.

[8]. Yang, K.; Ren, J.; Zhu, Y.; Zhang, W. Active Learning for Wireless IoT Intrusion Detection. IEEE Wirel.Commun. 2018, 25, 19–25.

[9]. Erhan, L.; Ndubuaku, M.; Mauro, M.D.; Song, W.; Chen, M.; Fortino, G.; Bagdasar, O.; Liotta, A. Smart Anomaly Detection in Sensor Systems: A Multi-Perspective Review. Inf. Fusion 2021, 67, 64–79.

[10]. Jeon, J.H.; Kim, K.H.; Kim, J.H. Blockchain based data security enhanced IoT server platform. In Proceedings of the International Conference on Information Networking, Chiang Mai, Thailand, 10–12 January 2018; pp. 941–944.

[11]. Suhail, S.; Hong, C.S.; Lodhi, M.A.; Zafar, F.; Khan, A.; Bashir, F. Data trustworthiness in IoT. In Proceedings of the International Conference on Information Networking, Chiang Mai, Thailand, 10–12 January 2018; pp. 414–49.

[12]. Kshirsagar, D.D.; Sale, S.S.; Tagad, D.K.; Khandagale, G. Network Intrusion Detection based on attack pattern. In Proceedings of the ICECT 2011-2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011; pp. 283–286.

[13]. Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access 2019, 7, 31711–31722.

[14]. Moustafa, N.; Turnbull, B.; Choo, K.R. An Ensemble Intrusion Detection Technique based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet Things J. 2018, 6,4815–4830.

[15]. Bagaa, M.; Taleb, T.; Bernal, J.; Skarmeta, A. A machine learning Security Framework for Iot Systems IEEE Access 2020, 8, 114066–114077.