A Smart Framework to Detect Threats and Protect Data of IoT based on Machine Learning

Ahmad Alkheder Almasabi *

Posted Date: 26 September 2023

doi: 10.20944/preprints202309.1742.v1

Keywords: Internet of Things (IoT), Security, Machine Learning, Fog computing,

Article

A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning

Ahmad M. Almasabi [1,3,*], Maher Khemakhem [1,*], Ahmed Harbaoui [1], Fathy Eassa [1], Ahmad. B. Alkodre [2], kamel Jambi [1] and Adnan Ahmed Abi Sen [2,*]

[1] Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] College of Computer Science – Islamic University – Madinah – KSA
[3] College of Computer Science & Information System, Najran University, Najran, KSA
* Correspondence: amalkheder@nu.edu.sa; makhemakhem@kau.edu.sa; adnanmnm@iu.edu.sa

Abstract: The Internet of Things (IoT) has witnessed rapid and widespread adoption across various domains, including transportation, healthcare, education, agriculture, urban planning, smart homes, and more. Despite its transformative potential, this pervasive deployment of IoT devices has introduced new challenges, particularly concerning security and privacy threats such as unauthorized data access and device breaches. The excessive usage of these technological devices, coupled with the absence of robust security and privacy systems for user data, calls for a comprehensive approach to address these issues. In this study, we propose a novel framework designed to analyze, audit, test, and detect potential vulnerabilities within IoT environments and applications. The central components of the proposed framework include a machine learning algorithm for data classification and attack detection, along with the integration of Blockchain technology to enhance security measures. Specifically, the framework performs an in-depth analysis of user data to identify potential security or privacy vulnerabilities. Additionally, it conducts rigorous testing of smart services and automated data-collecting devices. To evaluate the effectiveness of our classification algorithm, we conducted a comprehensive implementation on a real-world IoT dataset. The results showcased the efficiency and accuracy of our approach in detecting and mitigating potential threats. Furthermore, based on our research findings, we provide valuable recommendations for enhancing security and privacy in IoT ecosystems. We also highlight emerging trends in the security and privacy domains, which can serve as valuable insights for researchers and practitioners. In conclusion, our proposed framework offers a robust and proactive approach to address the security and privacy challenges, such as unauthorized data access and device breaches posed by the widespread adoption of IoT devices. By combining machine learning algorithms and Blockchain technology, we contribute to safeguarding user data and fostering a secure environment for IoT applications. This study lays the groundwork for further advancements in the realm of IoT security and privacy, ensuring a safer and more resilient IoT landscape for the future.

Keywords: Internet of Things (**IoT**); Security; machine learning; fog computing

1. Introduction

IoT is a technological revolution revealing the potential connectivity and reachability for the future. The information and communication systems have been altered significantly via the upcoming advent of IoT technology and cloud computing. Resource distribution through multiple clouds and the involvement of various heterogeneous devices are consequences of the IoT-based revolution. IoT and Cloud computing have introduced a novel logistic service mode. In this regard, virtualization will boost cloud computing security (Figure 1 depicts main layers of IoT) [31].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

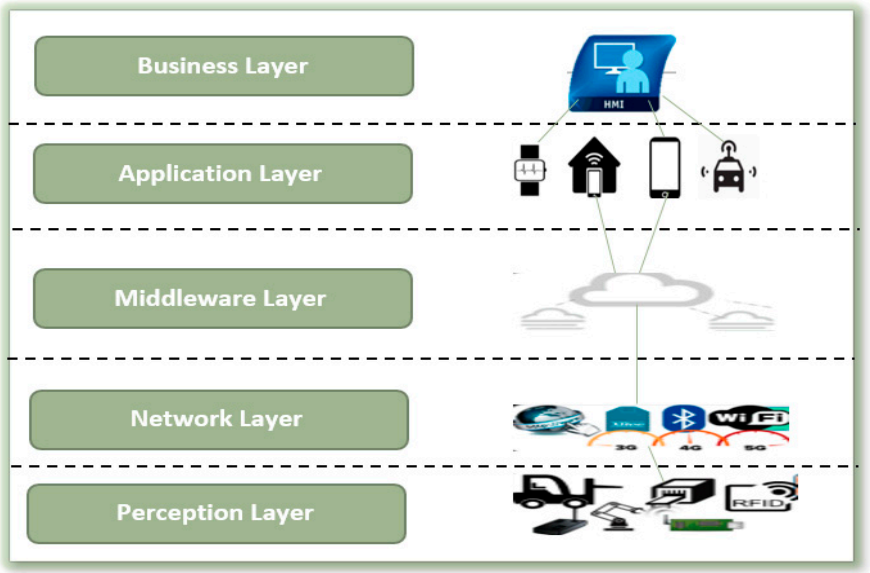

Figure 1. Five Layers IoT Architecture.

IoT meets between the concepts of "Internet" and "Things" as it is defined. Connected objects are connected globally via addressable unique standard communication protocols. Moreover, a smart context-sensitive web connects several things to be controlled distantly, recognized, and sensed via smart actuators and sensors. In an IoT environment, each physical object has a virtual actor representation, so they can communicate, act, interact, sense, and exchange information, knowledge, and data. The physical world information data is collected via IoT devices and transferred into the virtual world among tremendous applications. A substantial significant volume of IoT data is generated rapidly via more and more sensors growing very fast [32].

Novel new paradigms involving cloud computing, big data, IoT, and Blockchain are coined to permit information access and remote storage [1]. IoT depicts as though entities and things are interconnected with each other. Moreover, objects through the network could be monitored remotely and near the web with less human intervention. IoT introduces versatile transformation of objects and transfers them from conventional into intelligent devices via specific techniques such as data science, cloud computing, telecommunication, and others. It assists in correctly managing the power management of the home to permit consumers to be part of the revolution as the Internet revolution and emerging. Furthermore [2]. IoT provides billions of applications in different majors like Health, Transportation, Learning, Energy, Crowd, to name a few [33,34].

However, in IoT security, confidentiality is essential to protecting information from breaches during data transmission to verified nodes [3]. The critical step to keeping confidentiality is cryptographic measures which measures and defenses network communication [4]. Integrity in IoT ensures information is not modified from senders during data transmission and avoids any collision from radio wave propagation. Besides other IoT security, Availability of IoT is the survival service at all network layers. Due to the prevalent use of IoT globally, availability is the first of the security requirements list [3]. Authenticity in IoT is a manner to verify the correct identity device in an IoT network to ensure network safety and avoid disturbing the entire model. In non-repudiation, a sender is in charge of data sending and receiving acknowledge of the same receipt [4]. This standard has a significant role in IoT security to detect and prevent malicious nodes from sending misinformation [5].

Security of the Internet of Things (IoT) has a tangible role in avoiding any shortage of supply or errors. The versatility of IoT among various application areas such as wearable technologies, the smart system of transportation, home automation, and cars is altering the global world and making the best management progress. There was an estimation that there would be 30 billion IoT devices by 2020 with wireless communication, limited processing and memory, and less cost [6]. Several studies have announced that IoT networks are confronting diverse security threats and challenges

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

involving leakage of information, privacy, authorization, authentication, jamming, tampering, verification, eavesdropping, etc. [6]. IoT environment offers interoperable communication protocols and software tools with network infrastructure to enable the Internet connection of intelligent devices [7].

Wireless Sensor Networks (WSNs) have an emerging paradigm for IoT networks, and it is utilized in a prevalent range of application domains. WSN is deployed for specific applications for support purposes. On the other hand, for several IoT devices, connected mobile platforms offer global connectivity for tremendously diverse applications. WSN nodes have prevalent use and are very powerful in determining that several applications share the same WSN infrastructure. This sharing could be prospectively applicable via virtualization technology (Figure 2 shows different classes of WSN) [10].

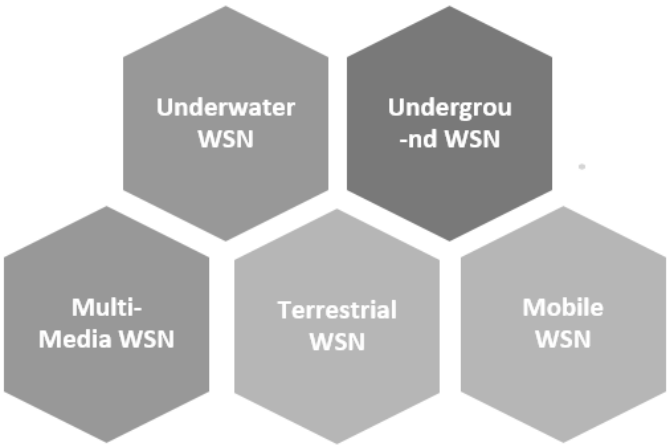

Figure 2. Classifications of Wireless Sensor Nodes.

Tracking, killing tags, reverse engineering, cloning, viruses, block tag, and side-channel are diverse kinds of attacks compromising the RFID physical system. The previous attacks are applicable due to low resources in RFID devices and weak encoding schemes. The feasible suggestion to solve and overcome these vulnerabilities is to involve access control, data encryption, and cryptography techniques to secure any side-channel attacks and to use hashed-based access control and cipher text re-encryption to hide communication. GPS sensors also consider vulnerable to jamming or data-level and signal-level spoofing resulting in Time Synchronization Attacks (TSAs). A feasible countermeasure for these kinds of vulnerabilities is the node's authentication and privacy techniques for sensors [35].

It was not easy to mitigate intrusion risk in IoT devices. Security degree requires protection at each level to prevent an attacker from achieving his goals and involving all members, from manufacturers to consumers to lawmakers, to cooperate and understand the consequences of the security threats. Another risk mitigation is finding new methodologies to outgrow the market shortcomings from the ground up abreast in security and privacy perspective [36]. There are a variety of practices and solutions available in the present IoT security and privacy landscape targeted at reducing the always changing dangers. These consist of numerous authentication methods, access restrictions, and encryption approaches. However, it is clear that as IoT networks grow and become more diverse, they face more complicated and dynamic difficulties. IoT ecosystems may not be sufficiently protected against new threats by traditional security techniques. The goal of our suggested framework is to address this urgent need for novel methods to strengthen the security and privacy of IoT devices and networks [36].

2. Contributions

This paper aims to address the security and privacy challenges in the IoT environment comprehensively. We propose a novel approach that combines Machine Learning algorithms and Blockchain technology to enhance security while preserving user privacy. Our approach focuses on

 doi:10.20944/preprints202309.1742.v1

ensuring Confidentiality, Integrity, and Availability (CIA) in IoT devices, as well as hiding user's personal information and preventing data tracking. Furthermore, we emphasize the need for security awareness among developers and end-users and advocate for rigorous legislation and incentives to promote secure IoT practices. Additionally, we highlight the importance of novel, stringent security and privacy solutions to counter the growing threats posed by resource constrained IoT devices. Our contributions strive to pave the way towards a safer and more privacy conscious IoT ecosystem. ML and proposed algorithm will enable the framework to detect any security threat then dealing with it. By integrating these contributions into the introduction, the paper presents a complete and coherent overview of the IoT landscape, its security challenges, and the proposed approach to address them.

***Main Contributions*:**

- Build a comprehensive framework to detect the security and privacy threat based on ML.
- The framework focuses on the triple security properties (CIA).
- The framework provides an idea for dynamic protection in IoT systems based on the detected threat.
- Provide enhanced IoT dataset to enhance the accuracy of the proposed classification algorithm.

The subsequent sections of this article will follow a structured outline: first, we will delve into three fundamental concepts - Blockchain, IoT Architecture, and various machine learning algorithms. Next, we will conduct a comprehensive literature review to provide insights into prior research and related works. Following this, we will present the intricacies of our innovative hybrid framework architecture. Subsequently, we will offer a detailed analysis of our research findings and results. Finally, we will conclude by summarizing the key takeaways from our work and delineate potential avenues for future research.

3. Materials and Methods

3.1. The Blockchain Technology

In Blockchain technology, a local private blockchain has a policy header to ensure the following users' policy for incoming and outgoing transactions and track their transactions. Commencing from the genesis transaction, all device transactions are linked together as an immutable ledger in the Blockchain. Each block in the local Blockchain has a block header and policy header that is used to authorize devices and keep following the owner's control policy. In contrast, the block header involves the former block hash to ensure the Blockchain is immutable [8]. Moreover, the policy header involves four parameters: The Requester parameter indicates the PK requester in a received overlay transaction. Second, a parameter in the policy header refers to the requested transaction action, which can either be stored data locally or stored data to the cloud, accessed, or monitored to access real-time data. The third is the smart home device ID; the fourth is the transaction's action matching the former properties [8].

Furthermore, the header involves five parameters stored in the local Blockchain: the first two is utilized to chain the same device transaction to identify each transaction uniquely in the Blockchain. A third parameter is the ID of the transaction's corresponding device. Next is the transaction type to reveal genesis, access, store, or monitor transactions. The fifth parameter is stored if the transaction comes from an overlay network; otherwise, will be free blank.

Machine learning is a field of computer science algorithms to sophisticate via experience and via data use automatically without human being intervention. Machine learning techniques involve two kinds: supervised learning, where the predictive data model is based on input and output data, and it has two kinds of classification and regression. The second type is unsupervised learning, where interpreting data is based on input-only data and has one type: clustering. Leveraging machine learning's capabilities to improve security within the Blockchain network is how Blockchain and machine learning are related to preventing data leakage. By enhancing encryption, finding abnormalities, limiting access, monitoring in real-time, and examining user behavior, machine learning makes a contribution. A more reliable and secure mechanism for preventing data leakage

 doi:10.20944/preprints202309.1742.v1

and ensuring data secrecy within the Blockchain is created as a result of this collaborative approach [37].

We use Blockchain technology to build an impenetrable fortress that prevents data leakage due to sniffer attacks, which involve unauthorized access to network traffic in order to intercept data. An attacker uses a sniffer attack to eavesdrop on data packets as they are sent over a network, potentially gaining access to sensitive data. By offering a safe and impenetrable method of storing and sending data, assuring the highest level of security, Blockchain technology is used to thwart such attacks.

3.2. IoT Architecture

The five layers of IoT architecture involve the perception layer, Network layer, Middleware layer, Application layer, and Business layer [38].

The perception layer where Data is gathered from IoT devices with limited resources, involves IoT devices deployed with low-power and loosely networks (LLNs) where energy, processing power and memory are constrained compared with local network nodes in conventional Internet. Associating secure public key encryption-based authentication schemes is unreasonable since the demand significant computational power and storage capacity. Hence, establishing a cryptographic protocol will be challenging for scalability, ease of deployment, and context-awareness. So, specific problems will arise in this perception layer [39].

In addition, the network layer, that manages device-to-device communication and data transmission, is in charge of the intermediate layer between the perception layer and the middleware layer. The middleware layer has the responsibility to gather information, processes storing and analyzing data before passing it to applications. In the business layer, it defines IoT application change and management. This layer establishes the strategies, regulations, and administration of IoT applications. Fog computing plays a critical role in this layer by the integration with the cloud computing [40].

The application layer of IoT involves several applications and transfers them to users. Possible attacks on this layer could be software-based attacks or encryption-based attacks. Software attack relies on malicious software agent, such as impersonating a trusted authority to reveal the user credentials of authentication. Malware (viruses, worms, Trojans, ransomware), spyware, adware, impersonation attacks, data manipulation attacks, privilege escalation attacks, and denial-of-service (DoS) assaults are all examples of software-based threats in the application layer of IoT. These assaults have the potential to have a considerable impact on IoT applications and their users [41].

Malware, for example, might disable device functioning, steal critical data, or hold devices hostage. Spyware violates user privacy by collecting sensitive information, and adware disturbs user experiences by displaying intrusive advertisements. Impersonation attacks dupe users into unauthorized interactions, and data manipulation attacks produce false data, potentially leading to wrong actions. Attacks on privilege escalation can offer unauthorized access, and DoS attacks can interrupt routine processes. It is critical to protect against these threats in order to protect user data, device operation, and overall IoT system integrity. The most prevalent occurrences in IoT application heterogeneity are malware, adware, spyware, worms, and Trojans [42].

In brief, IoT systems' overall functionality and security may be impacted by the limitations of IoT devices, particularly their finite resources, as well as the difficulties of putting cryptographic methods into practice. Resource optimization and security must coexist in harmony for IoT installations to be effective. Security measures, threat models, and risk evaluations that are suited to the particular IoT application and device capabilities are frequently carefully taken into account.

4. Related Work

The authors of [11] have introduced Sensor Function Virtualization (SFV) to perform distributed intelligence in an IoT environment. The authors also have declared certain limitations of the current IoT network, suggested that some of these limitations could be addressed by distributed intelligence, and discussed the advantages of SFV for IoT networks. However, their studies lack specific experiments to assess energy consumption reduction and the time delay.

 doi:10.20944/preprints202309.1742.v1

The author of [12] Lin has announced specific firmware and software vulnerabilities because of the absence of reliable cryptographic measures within the up-gradation phase. Around 60% of IoT devices are subject to software and firmware vulnerabilities. In addition, the author has stated that tremendous IoT devices such as webcam and power remote do not perform authentic passcode to get access; besides, the password or the passcode is recovered with less an authenticated and authorized manner. These IoT devices impact more and more websites due to their very fragile and poor security implementation mechanisms are applied.

The authors of [13] have introduced systematic and virtualization review methods in IoT networks. They have discussed IoT virtualization methods and software-defined networking and revealed their classification in certain kinds of solutions. The classes are categorized into architectural, management, and security-based solutions. The authors also have involved other studies depicting function virtualization implementation for normal network function in a logical area.

Several initiatives to authenticate IoT devices have been done using Physical Unclonable Functions (PUF). "A PUF is an expression of an inherent and unclonable instance-specific unique feature of a physical object which serves as a biometric for non-human entities, such as IoT devices [14]."

The authors of [15] have introduced a credibility verification method to reveal how a verification via Blockchain technology. This framework is built with layers, intersect, and self-organization Blockchain architecture to ensure efficiency, security analysis, storage efficiency, response time, and verification. The experiments have been conducted to reveal this method's validity and satisfy the credible requirements performed via Blockchain technology. To accomplish credibility verification, the corresponding data is required to be generated based on the original IoT data communication through a data model to apply credibility verification. The credibility verification is built for accessed devices via building a credibility verification chain through BCS on the path. The added data for each device is the ID and private Key to distinguish between each device. The disadvantage of this method is that it still needs a method to protect the usability and credibility of IoT devices, and it still has security risks. In addition, once an attack has taken place on Primary Server, it can't verify all nodes' credibility, indicating that this method does not yet accomplish a complete decentralization. Moreover, in a high-scale IoT environment, it still involves problems determining which BCS node number to pick up and controlling the tree height, which still requires a certain degree of solution to optimize it.

The method of [16] analyses the use of Blockchain technology to preserve privacy and security in IoT environments. This method has introduced the stalker, a selfish miner variant, to prevent a node from publishing its blocks on the main chain. The stalker is malicious mining to prevent a specific miner from publishing its blocks. Every node performs TCP into its neighbors in the network layer. So, every transaction has its address, and the node involving the correct key could unlock it. Therefore, the above reason answers and ensures that the Blockchain guarantees a certain degree of privacy. The disadvantage of this method is that it still does not mitigate and reduce computation consumption.

The authors of [17] have provided a BC-related analysis approach and technologies in an IoT environment to cover several application domains. This approach discussed and introduced two patterns: data management and device manipulation. The disadvantage of this method is that it has a static solution that prevents taking advantage of full decentralization, so it does not mitigate and reduce the complexity overhead.

The integration approach of [18] has introduced and integrated Blockchain technology to ensure sensing data integrity, allowing device owners to afford a specific application that provides immutable log and permits for facilitated access with their devices once it is deployed across diverse domains, and providing real-time monitoring and rigorous control from end-user and devices and vice versa. The relevant result of this method reveals satisfaction in specific resource-constrained scenarios. The method solution achieved the practical and scalable requirements of an IoT network. It utilized a permission Blockchain, so communication among network entities appears fully trusted

 doi:10.20944/preprints202309.1742.v1

between them. The fancy of this method is hiding the transaction history and IoT device details except for authorized users. The disadvantage of this approach is that it does not yet address the overhead computation nor mitigate it. This solution method omits IoT devices in the Blockchain. Still, it has been replaced by a RESTful interface to manipulate a request from devices to enable and establish communication among devices and the Blockchain network.

The authors of [19] have investigated the Blockchain and IoT integration and have analyzed diverse embedded technologies among them. The authors have focused on technical and strategic perspectives of IoT restrictions, Blockchain weaknesses, Blockchain-IoT integration approaches, and solutions to defeat the implementation challenges. They have provided high-level knowledge to define the use of Blockchain use cases in IoT systems and networks. The disadvantage of this method is that it still considers not comprehensive analysis and resolution for IoT manufacturers to meet appropriate Blockchain requirements and restrictions in the integrations. Moreover, it still recommends Blockchain usage to eliminate hiring third parties, store devices' state, and organize several writers. Still, it does not associate arbitrary machine learning algorithms with enhancing the analysis.

The method of [20] involves a security module for IoT devices to mitigate malicious attacks via Blockchain integration. It consists of verification but is poor in sophisticating the level of security. The framework of [21] has an intelligent and secure architecture using deep reinforcement learning, so the system effectiveness is enhanced, but It is poor in privacy level sophistication. The authors of [17] have done integration of Blockchain and IoT via testing the related research in IoT and Blockchain, but It does not reduce the complexity level. Whereas in [18], the authors have integrated Blockchain in IoT to secure sensing data, it does not mitigate communication overhead.

This study paper [22] has introduced a mechanism of random time hopping sequence and random permutations to ensure data user integrity in IoT and hide validation information. One advantage of this method is that it introduced a formal security analysis for certain proposed protocols with low computational complexity in terms of performance [22]. Our hybrid framework's mechanism will involve a hashing technique to avoid arbitrary data tempering with Blockchain technology and a machine learning-based detection system to enhance the overall security system in the IoT environment and ensure high Integrity of IoT environment system.

This study has revealed three diverse Denial of Service (DOS) attacks to test the IoT system's availability. The attack tool was Kali Linux [23]. Specific advantages of this study are that commencing attack of DoS via Kali Linux, the attacker, on simple IoT system within diverse methods. Moreover, CPU utility, attack time, memory utility, and success attack rate are provided. In addition, several DoS attack comparison methods are revealed with certain factors affecting the attack performance being inspected [23]. Our methodology will involve fog computing with Cloud hierarchy to ensure Free-DoS attacks associating Blockchain with a machine learning-based detection system to avoid arbitrary DoS attacks and enhance the availability of IoT environment in the system as well.

In this research, [24] has merged two methods: Blind Third Party (BTP) and Blind Peers (BLP), to get a novel method known as Blind Approach (BLA) to protect data via decoding with intermediate to hide an ID sender. An advantage of this research method is that BLA has no problem with other approaches. Response time average is affected via BLA slightly increasingly. Our mechanism in our hybrid framework associates Blockchain and machine learning-based detection systems with decoding algorithms to protect IoT data and enhance the confidentiality of IoT environment systems.

The authors of [25] have proposed a hierarchical modelling framework to guarantee the availability and IoT security infrastructure. The modelling methodology-based is a hierarchical model of 3 layers/levels: it involves at the top level the Reliability Block Diagram (RBD) to observe the entire architecture of IoT infrastructure. At the middle level, there is a Fault Tree (FT) to provide details of the system architecture of member systems in IoT infrastructure. At the bottom level, continuous time Markov chain (CTMC) to monitor operative states details bottom subsystem transitions in IoT infrastructure. Specific advantages of this methodology are to reveal the framework

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

model feasibility in smart factory infrastructure, which involves Fog, Edge computing, and Integrated Cloud. FT, RBD, and CTMC models are developed completely, and security measures and availability are analyzed.

This paper in [26] concentrates on how Blockchain technology has enhanced the availability and prevented DoS attacks due to the stable decentralization of the Blockchain technique and secure architecture. One advantage of this is that it has displayed Blockchain-based Distributed Denial of Service solutions and has compared the former Blockchain-based methods against DDoS attacks and their analysis.

The authors of [27] have proposed a machine learning-based layer framework to detect the DoS attacks within the MQTT protocol and test the scheme on the protocol compliant with DoS attacks. The advantage is that the MQTT feature has high attack detection accuracy. The length and field size features have radically decreased the false-positive rates and become suitable for detecting IoT-based attacks. Our hybrid framework methodology is built in fog computing with Cloud-based hierarchy, Blockchain technique, and machine learning-based detection algorithms to guarantee high availability and avoid arbitrary DoS.

The authors of [28] have suggested a model of complex attack for falsifying sensing data. Afterward, they proposed a weighted sequential hypothesis test (WSHT) to enhance the detection accuracy of the prime user to reduce the sampling number, which involves a status-trust evaluation mechanism of data transmission to ensure the availability of sensing data as well as a test of sequential hypothesis. One advantage of this model is that its simulation results have proved that once diverse attacks are confronted, the WSHT requirements have less than regular WSHT for higher detection performance. Our hybrid framework focus on enhancing the integrity of the IoT environment system via associating hash algorithms, Blockchain techniques, and machine learning-based detection algorithms to avoid arbitrary data tempering in the IoT environment system.

The authors of [29] have introduced a rigorous framework to ensure confidentiality, authentication, and integrity during the sensed data collection throughout elliptic curve cryptography. The authors have informed that Wireless Sensors Networks have limited resources and get affected by various vulnerabilities and security issues [29]. A perfect suggestion to preserve privacy and confidentiality is to perform encryption regardless of what causes problems in terms of performance and time latency. Our hybrid framework methodology of confidentiality has taken advantage of Blockchain associating decoding algorithms and machine learning-based detecting algorithms to avoid arbitrary data leakage and ensure high confidentiality in IoT environment systems.

The authors [30] have introduced the 5G-based AI technique to enhance the confidentiality of the IoMT network by associating the Blockchain-based technique to prevent identity threats and enhance integrity. One discovering in this research is that it is subject to diverse types of attacks, such as Denial of Service, eavesdropping, and malware. Moreover, diverse vulnerabilities are associated with it, for instance, in privacy, security, and confidentiality. Several novel cryptographic techniques such as data encryption, access control, and identity authentication to sophisticate IoMT reliability and security devices.

Table 1. summarize the previous approaches contributions.

Key Findings and Contributions	Challenges Addressed	Methodologies & Techniques	Connection to IoT	Ref
Introduced Sensor Function Virtualization (SFV) for distributed intelligence in IoT. - Addressed limitations in IoT networks. - Advantages of SFV for IoT.	Lack of specific experiments for energy consumption reduction and time delay assessment.	SFV, Distributed Intelligence.	Yes	[11]
Identified firmware and software vulnerabilities in IoT devices. - Addressed security issues related to access control.	Vulnerabilities in IoT devices. - Security risks due to poor implementation.	Access Control, Security Vulnerabilities	No	[12]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

Introduced systematic review methods for IoT networks. - Categorized virtualization methods. - Classified solutions into architectural, management, and security-based categories.	Lack of decentralization in solution. - Complexity overhead.	Virtualization, Solution Classification	Yes	[13]
Presented a credibility verification method using blockchain. - Conducted experiments to validate the method. - Highlighted security risks and limitations.	Method needs further protection for IoT devices. - Lack of complete decentralization. - Problems in high-scale IoT environments.	Credibility Verification, Blockchain.	Yes	[15]
Utilized blockchain for privacy and security in IoT. - Addressed privacy concerns.	Method does not mitigate computation consumption.	Privacy, Security, Blockchain.	No	[16]
Integrated blockchain for data integrity in IoT. - Achieved practical and scalable requirements. - Ensured trusted communication.	Communication overhead not mitigated. - Lack of IoT device integration in blockchain.	Data Integrity, Permission Blockchain.	Yes	[18]
Investigated blockchain-IoT integration and analyzed embedded technologies. - Focused on technical and strategic perspectives.	Incomplete analysis and resolution for IoT manufacturers. - Lack of association with machine learning algorithms.	Integration Analysis, Blockchain Use Cases.	Yes	[19]
Introduced a security module for IoT devices using blockchain. - Addressed malicious attacks.	Low sophistication in security level.	Security Module, Blockchain.	No	[20]
Presented an intelligent and secure architecture using deep reinforcement learning. - Enhanced system effectiveness.	Low sophistication in privacy level.	Security Architecture, Deep Learning.	No	[21]
Proposed a mechanism for data user integrity in IoT using random sequences and permutations. - Ensured low computational complexity.	Mechanism slightly affects response time.	Data User Integrity, Random Sequences.		[22]
Demonstrated blockchain-based solutions for preventing DoS attacks. - Compared blockchain-based methods against DDoS attacks.	Emphasized stable decentralization.	DoS Attack Prevention, Blockchain.		[26]
Proposed a machine learning-based framework to detect DoS attacks in MQTT protocol. - Achieved high attack detection accuracy.	Improved false-positive rates	DoS Detection, MQTT Protocol.		[27]
Introduced a model for detecting data falsification attacks. - Proposed a weighted sequential hypothesis test (WSHT). - Enhanced detection performance.	WSHT requirements slightly affect response time	Data Falsification Detection, WSHT.		[28]
Established a framework for confidentiality in data collection using elliptic curve cryptography. - Addressed vulnerabilities in Wireless Sensor Networks.	Performance and time latency issues with encryption.	Confidentiality, Encryption.		[29]
Utilized 5G-based AI to enhance IoMT network confidentiality. - Addressed	Diverse security and privacy vulnerabilities.	AI, Confidentiality, Blockchain		[30]

 doi:10.20944/preprints202309.1742.v1

various types of attacks and vulnerabilities.

Brief, we are excited to present our cutting-edge Hybrid Framework Architecture as part of our unwavering effort to secure the Internet of Things (IoT). Our innovative strategy is intended to address security and privacy issues in IoT contexts, creating a new standard for security, privacy and fostering user trust. This work will not delve into the proposed framework completely. It will focus on security, we concentrate on addressing three types of security threats: data leakage, data tampering, and denial of service (DoS).

To tackle these challenges effectively, we employ specific techniques. Firstly, we utilize the decoding technique to discern data leakage attacks among IoT devices. Secondly, the hashing algorithm is deployed to identify data tampering attacks within the IoT environment. Lastly, fog computing integrated with Cloud hierarchy is employed to prevent arbitrary denial of service (DoS) attacks. Furthermore, our Blockchain manager plays a pivotal role in detecting various security threats and ensuring robust protection for the IoT system. By doing so, we mitigate the potential vulnerabilities within the IoT environment.

5. The proposed Hybrid Framework Architecture:

After investigating most former research on security and privacy attacks in IoT environment systems, we have observed none of them have introduced a comprehensive hybrid framework detecting both security and privacy at the same time simultaneously, nor did they propose a dynamic detection methodology for both safety and privacy together. In this research, we will introduce a hybrid framework to detect and measure a total of 6 threat attacks, 3 of them are for security attacks, and three are for privacy attacks to be protected from them in the IoT environment system and provides dynamic protection for each of these kinds of attacks. The Blockchain will be associated with this hybrid framework to guarantee the security level requirements: Confidentiality, Integrity, and Availability with decoding the IoT data since the Blockchain ensures all linked nodes are connected securely without arbitrary modification of IoT data.

Blockchain will be associated more with the three security attack kinds. Since it is not rigorous enough alone, we will aside associate hashing techniques for integrity, decoding in confidentiality, and fog computing with the cloud hierarchy to guarantee availability and avoid arbitrary DoS attacks. In terms of privacy requirements: Identification, Tracking, and Profiling. In general, we will take advantage of a machine learning-based detection system to detect these privacy requirements; Besides, Obfuscation will be suggested to be associated in this hybrid framework to avoid arbitrary tracking attacks, whereas dummy and swap cooperation would be associated to ensure free-profiling attacks of user data as well as to prevent theft identity attacks.

Moreover, most research has not focused on sensors in wireless network sensors, such as sinkhole node attacks in which it just receives data and not sends them, annoys the surrounding nodes, or even sends misinformation to other nodes. Therefore, machine learning is a suitable solution that will be integrated with our hybrid framework to detect, measure, and address certain kinds of these attacks.

Briefly, we describe our proposed method for enhancing security and privacy on the Internet of Things (IoT) environment in this part. To solve numerous security and privacy concerns in IoT systems, our suggested hybrid framework architecture combines cutting-edge technologies including blockchain, fog computing, and machine learning-based detection systems. Our approach strives to protect user data, prevent unauthorized access, and quickly identify and neutralize potential threats by integrating these potent capabilities. The main contribution in this work is the proposed algorithm based on ML to early detect threats in IoT environment especially WSNs applications, in addition to an initial idea of dynamic and adaptive protector for privacy and security threats and attacks.

Let's explore each element's specifics and how they work together to form a solid and dependable IoT security and privacy framework. Figure 3 illustration offered illustrates a proposed

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

security and privacy architecture, showing numerous essential elements properly incorporated into the system.

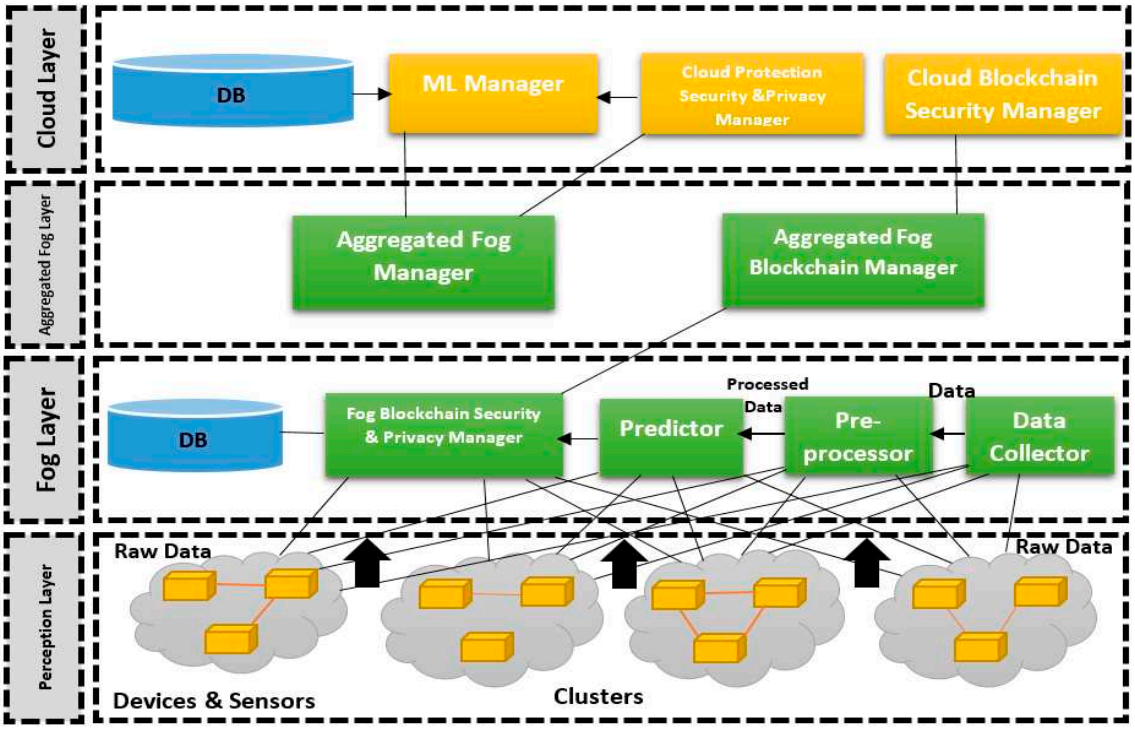

Figure 3. The proposed Architecture of Hybrid Testing and Protection Framework.

5.1. Perception layer

Before being uploaded to the Aggregated Smart Blockchain Manager, data gathered from IoT devices in the Perception Layer.

5.2. Fog Layer

Three crucial components make up the fog layer. The preprocessor deals firstly with collected data, removes repeated, does some statistics. Then the Predictor recognizes and categorizes IoT device behaviors in addition to discriminate between typical and abnormal patterns based on the machine learning algorithms. The predictor acts the Malware Preventer which examines the outcomes of possible attacks on IoT data. Then the Blockchain Manager proactively limits some assaults before they reach the Cloud Layer, effectively reducing the processing load on the cloud. This manager effectively manages a large amount of IoT data by utilizing encryption and hashing methods.

5.3. Aggregation Layer

The Fog manager is responsible about manage the fog nodes in the fog layer based on the created knowledge in the cloud. While the Aggregated fog blockchain manager represents the master nodes of blockchain which responsible on validated data and consensus algorithms.

5.4. Cloud Layer

The Cloud Layer plays a vital role in integrating blockchain and machine learning algorithms. Utilizing the Blockchain's trust data and distributed storage capabilities, it facilitates secure and reliable data handling. Machine learning models operating within this layer contribute to automated consensus, enabling efficient decision-making based on analyzed information. Moreover, ML manager trains on the stored big data to find rules and knowledge which distributed on the fog nodes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

5.5. Integration of Machine Learning

Within our proposed framework, machine learning plays a critical role in improving threat detection capabilities. Machine learning algorithms will be painstakingly trained on historical and real-time IoT data to identify numerous patterns and abnormalities indicative of security and privacy issues. These algorithms will be subjected to continual learning and adaptation, assuring their ability to detect evolving threats over time. They will be specifically intended to detect patterns associated with security breaches, privacy violations, and questionable activity inside the IoT ecosystem. During the training phase, the algorithms are exposed to a variety of datasets, allowing them to autonomously modify their detection criteria depending on developing threat profiles. This continuous adaptation maintains the framework's robustness and responsiveness to the ever-changing landscape of IoT security and privacy problems.

5.6. Benefits and Advantages:

This hybrid approach offers several distinct advantages

5.7. Dynamic Protector

The Dynamic Protector, a crucial component of the Hybrid Framework Architecture, serves as the framework's immediate response mechanism. Its key goal is to respond quickly to threats in order to safeguard the security and privacy of the IoT ecosystem. This component employs targeted defense strategies adapted to the type of threat, ensuring robust digital security and privacy across the IoT ecosystem. It offers comprehensive defense by efficiently addressing both privacy and physical security concerns. In this research, our primary focus is on the detection algorithm rather than the protection mechanism. For protection, we rely on the blockchain to secure data and implement certain physical actions, such as disconnecting or exposing nodes, to deal with malicious node issues and their attacks (Figure 4). However, in our future work, we will present the proposed technique to address privacy concerns. Table 2 and Figure 5 illustrate some of the actions taken in response to detected attacks, while Table 1 provides a few solutions for security and privacy issues categorized by the type of threat.

Table 2. Summary of Benefits and Advantages of this Hybrid Framework.

Key Advantages	Description
Comprehensive Threat Detection	To provide full threat detection capabilities, our framework incorporates cutting-edge technologies such as Blockchain, fog computing, and machine learning-based detection methods. This means it can detect and respond to a wide range of security and privacy concerns at the same time.
Dynamic Adaptation	Unlike many existing solutions, our framework incorporates machine learning algorithms that constantly adapt and learn from shifting threat landscapes. This dynamic method ensures that the system stays successful in detecting emerging threats, making it more resilient to new attack vectors.
Privacy Protection	Beyond security, our system prioritizes user privacy. It protects sensitive data and reduces tracking and profiling attempts by incorporating obfuscation techniques and identity theft protection measures.
Resource Efficiency	By using fog computing to preprocess and filter data before it reaches the cloud layer, the architecture optimizes resource utilization. This lessens the processing strain on cloud servers while improving overall system efficiency.
Scalability and Flexibility	The suggested hybrid framework is built to scale smoothly as the IoT environment expands. Its adaptability enables simple integration with a wide range of IoT devices and network setups, making it appropriate for a wide range of applications.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

Decentralized Security	Our system offers decentralized security by leveraging blockchain technology, making it resistant to single points of failure and unauthorized data revisions. This improves the integrity and availability of data.
User-Focused	Finally, our approach prioritizes user data security, secure access management, and rapid threat response. This user-centric design reduces the possibility of unauthorized data access and ensures that IoT environments are secure and trustworthy.

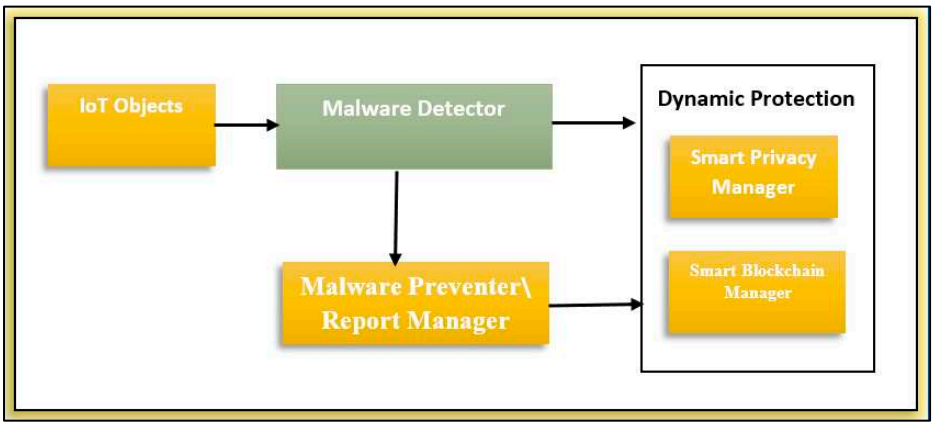

Figure 4. A proposed general security and privacy architecture framework based on Blockchain Integration.

Table 3. Integrated techniques of detection and protection in Hybrid framework**.**

Threat Concern	IoT Attack type	Security Requirement Target	General Integration Techniques	Associated in Our Framework
Security	Data leakage - Sniffing	Confidentiality	Machine Learning and Blockchain	Decoding
Security	Data Tampering	Integrity	Machine Learning and Blockchain.	Hashing
Security	(DoS)	Availability	Machine Learning and Blockchain.	Fog Computing with Cloud.
Privacy	Linking data	Profiling	ML-based Detection System	Dummy - Swap cooperation
Privacy	Identity Theft	Identification	ML-based Detection System	Dummy - Swap cooperation
Privacy	Tracking attack (Location)	Tracking	Machine Learning	Obfuscation

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

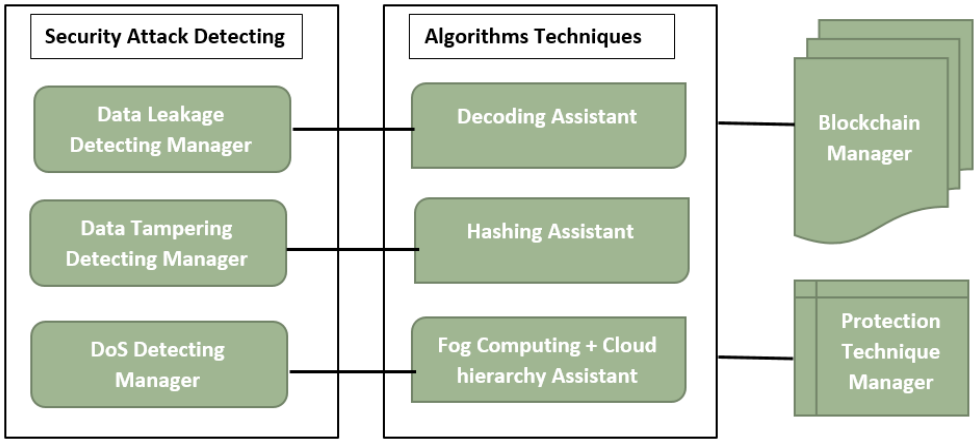

Figure 5. Proposed Security Threats and Techniques in the Hybrid Framework.

6. The Model of Machine Learning for the Hybrid Framework

Figure 6 shows the main steps followed in the proposed threat detection and classification algorithm based on machine learning model. In the training phase, features are collected and identified, then trained and tested to create the model that will be relied upon in the classification process. In selecting features in the IoT environment, it is usual to rely on the following features:

Timestamp, Sensor Type, Value, Date, Time, Data Size, and Class (Yes represents a threat, or No there isn't)

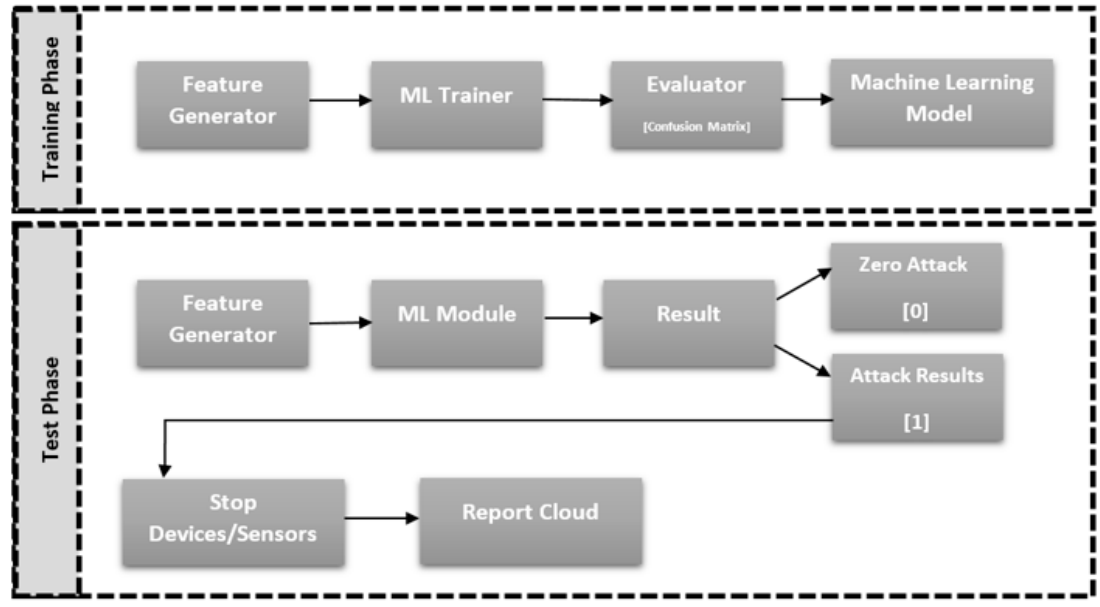

Figure 6. The Model of Machine Learning for the Hybrid Classification Framework.

The threat detection machine learning models are trained using multiple features retrieved from the IoT environment data. These characteristics are essential for effectively categorizing threats. Timestamp, Sensor Type, Value, Date, Time, Data Size, and Class (showing whether or not a threat is present) are typical attributes. In addition, we have included two new features to improve classification accuracy and threat nature identification.

In the proposed algorithm, we have added two additional features to improve classification accuracy on the one hand, and on the other hand to enable the algorithm to determine the nature of the threat itself. The first advantage is the time difference between the last and previous operation, in other words, the time delay in the transmission process. The second feature is the difference between the sensor value and the previous value, in other words, the amount of change in the sensor value.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

Note that using Fog Node made it possible to prepare the data in the appropriate manner, especially the two additional features.

In order to pick up the best model for machine learning, four famous models were tested:

- Support Vector Machine (SVM)
- Logistic Regression (LogR)
- K-Nearest Neighbor (KNN)
- Deep Learning (DL)

These models were selected based on their potential to provide accurate threat classifications and their suitability for handling IoT environment data.

The results of threat classification are analyzed to decide the best course of action. When a danger is positively categorized, appropriate mitigation activities are taken. For example, detecting a significant variation in sensor data may suggest sensor tampering or hacking, requiring measures such as sensor disconnection or exposing nodes to handle malicious node concerns and associated assaults.

The fog node will pre-process the features and use them as input for the learning model, which will then classify the data during the testing phase. A positive classification indicates the presence of a threat requiring a specified response.

Significant value differences could suggest a sensor malfunction or vulnerability to data manipulation. A large delay number, on the other hand, may indicate a Denial-of-Service (DOS) assault aiming at disrupting the service. The sensor should be deactivated in the first situation, and a backup availability policy should be applied in the second.

The following code explains how the proposed algorithm works:

```
import Library (pandas pd, numpy np, matploat plt, and sklearn)
url="IoT_Thermostat_End3.csv" # Dataset
from google.colab import files # Upload Dataset File to Cloud
uploaded = files.upload()
Features =
['date_d','date_m','date_y','time_h_m','time_s','current_temp','value_change','t_delay','class']
print ('shape of dataset')
print(dataset.shape)
print(dataset.describe())
X = Features [1:,0:8] # All rows of cols (start from 0 until 8-1 cols) as input
Y = Features [1:,8] # All rows of the col 8 is the Output
#Divide data to Training (30%) and Testing (70%)
x_train, x_test, y_train, y_test = model_selection.train_test_split(X, Y, test_size=0.3, random_state=7)
#Using Smote for imbalanced Issue
smote = SMOTE ()
x_smote, y_smote = smote.fit_resample (X, Y)
x_train, x_test, y_train, y_test = model_selection.train_test_split(x_smote, y_smote, test_size=0.3,
random_state=7)
#Apply ML models
model = KNN ()
model.fit(x_train,y_train)
predictions = model.predict(x_test)
model = SVC ()
model.fit(x_train,y_train)
```

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1


```
model = LogisticRegression()
model.fit(x_train,y_train)
model = Sequential () #Deep Learning
# Number of layers, in addition to select activation and optimizer models
model.add(Dense(12, input_shape=(4,), activation='relu')) # 4: number of X
model.add(Dense(5, activation='relu'))
model.add(Dense(1, activation='sigmoid'))
model.compile(loss='binary_crossentropy', optimizer='adam', metrics=['accuracy'])
history = model.fit(X, Y, epochs=150, batch_size=10, verbose=0, validation_split=0.3) #,shuffle=True
# Draw Accuracy Curves (training and validation)
plt.plot(history.history['accuracy'],'r',linewidth=3.0)
plt.plot(history.history['val_accuracy'],'b',linewidth=3.0)
# For each Model find the Confusion Matrix to calculate the Accuracy, Precision, Recall, and F1-Score
print('KNN Smote',accuracy_score(y_test, predictions))
matrix = confusion_matrix(y_test,predictions, labels=[1,0])
tp, fn, fp, tn = confusion_matrix(y_test,predictions,labels=[1,0]).reshape(-1)
print('Confusion matrix : \n',matrix)
```

The code snippet provided is critical in the threat detection process. It measures the rate of change between past and current sensor values, the transmission time delay, and data size. It evaluates whether or not a danger exists based on these metrics and the output of the machine learning model.

Note1: The change-rate is affected by the previous value or other sensors, whereas the delay-rate is the time difference between the current and prior measurements. The inclusion of these features improves the algorithm's accuracy.

Note2: implies that utilizing multiple machine learning models for increased accuracy is conceivable, such as depending on the best three models' consensus to make judgements.

Usually, sensors send each 6s, then service providers build their time series by collecting data for specific duration. Most of the previous algorithm depends on the time series and history of attacks to predict any new attacks. These methods did not achieve high accuracy in prediction or classification. For that, this research suggested adding additional features to time series which are change-rate and delay-rate. Moreover, we separated the work into 2 sections. First will be on detect attack on data between sensors and devices in fog layer, and next phase will process between fog and cloud data or service providers.

Traditional algorithms often rely on historical data and time series analysis to predict and classify new attacks. However, these methods may not achieve high accuracy. In contrast, our proposed method focuses on identifying anomalies in sensor data, especially change-rate and delay-rate, to detect potential threats in real-time, reducing reliance on historical context.

The maid idea of our proposed method is to detect various forms of threats, such as manipulation, hacking, data tampering, or denial of service, by identifying substantial deviations in sensor values, transmission speed, and data size. The work is divided into two parts, the first of which addresses risks between sensors and devices in the fog layer, and the second of which processes data between the fog and cloud, enabling total threat detection and defence.

Next section discusses the implementation and results of the proposed algorithm. As a fundamental dataset, we used the TON_IoT dataset in our research. However, we tailored this dataset to our suggested strategy, adding additional features and data processing techniques to improve threat detection and classification accuracy.

7. The Results Discussion

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

To test the proposed classification algorithm for detecting the presence of an attack or not in real time, it was implemented on a dataset of a set of different sensors, which were formed by "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems" [43].

Python language was relied on Google Colab platform to implement the proposed algorithm. In the basic TON_IoT Paper, training, testing, and detection of the attack were relied on several criteria: date, time, and sensor type, which explains the low accuracy of the results achieved by the previous Paper, despite the experiment on different types of machine learning models, which did not exceed 77%. Therefore, in this work, we have employed the fog node to play another effective role in adding three important criteria to the six basic data.

The first criterion is the time difference per second (the delay) between the last transmission and the previous one. In addition, While the second criterion is the difference of the sensor value itself between the last transmission and previous transmission. It is known that some sensors such as temperature, for instance, do not directly change the value, and most of the sensors send their data on a semi-constant periodic basis. Therefore, the large difference in transmission periods indicates in some types of sensors the presence of an attack or a physical defect. In short, these two criteria have been added to the data set to become as shown in Figure 7.

ID	Type	Value	Time	Date	Value difference	Time difference	Size	Class
1	Temperature	32	10:12:34	22-12-22	0	6s	2b	0 Normal
1	Temperature	32	10:12:40	22-12-22	0	6s	2b	0 Normal
1	Temperature	32	10:12:46	22-12-22	0	6s	2b	0 Normal
1	Temperature	32	10:12:55	22-12-22	0	9s	2b	1 Attack
1	Temperature	15	10:13:02	22-12-22	17	6s	2b	1 Attack
1	Temperature	32	10:12:08	22-12-22	0	6s	2b	0 Normal
1	Temperature	60	10:12:14	22-12-22	28	6s	2b	1 Attack

Figure 7. Dataset's Shape with Samples data.

Note that Class feature is a binary variable, where 1 indicates an attack or threat, and 0 indicates no threat. Initial processing was carried out for some of the data in which the date or time was incorrectly formatted, then the undisciplined data or those containing incomplete values were deleted.

Eventually, a clean base data containing 5000 readings of the temperature sensor was obtained. In the beginning, three common classification machine learning models were selected to test the proposed algorithm on the data set that was formed. These models are:

- K Nearest Neighbor (KNN)
- Support Vector Machine (SVM)
- Log Regression (LR)

The best achieved accuracy result was 94%, but we noticed by reviewing the confusion matrix that the data was not balanced, meaning that the cases that were classified as a threat constituted 33% of the results, while the other 67% were classified as healthy. To solve the balance problem, the SMOTE function was relied upon, and it intelligently generates additional samples based on the existing samples, instead of duplicating or doubling the same samples or deleting some samples of the section with the largest percentage.

Figure 8 depicts a comparison of the results before and after equilibration of the samples, so the Confusion matrix was as [[485 56], [28 931]], and the Accuracy was 94%. After applying the SMOTE Function, the Confusion matrix becomes balanced as [[867 44], [56 877]], and the Outcome values of TP FN FP TN: 867 56 44 877 respectively and the Accuracy increased to 95%.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

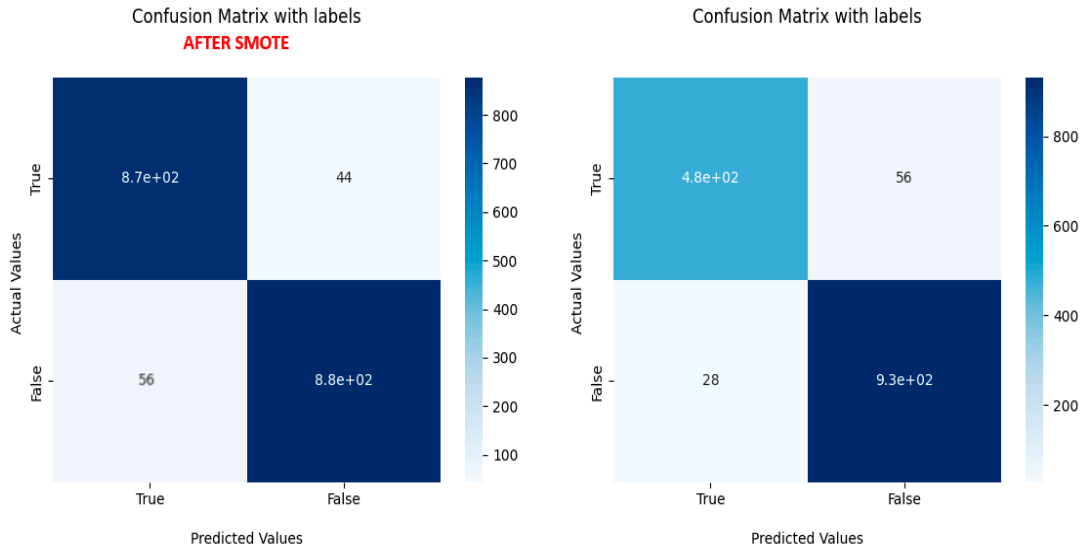

Figure 8. Confusion Matrix before and after using SMOTE for unbalancing issue.

After implementation on the three models, the highest accuracy achieved was 0.964 for the SVM model. Moreover, our Learning Curve grants weren't good enough to guarantee solid results on real, untrained data. Therefore, the deep learning model was added as an additional learning model, and we obtained an accuracy result of 99% with a satisfactory training curve.

Therefore, this model was adopted to be placed within the fog node to perform an automatic classification in real time for each value after reshaping it as an input to the model. If a threat is detected, the fog node will stop dealing with the attacked sensor and send an alert or a report to the user.

Figure 9 shows a comparison between the values of the Confusion Matrix for each model and shows the values of the famous criteria in the comparison between classification models, which are: Accuracy, Precision, Recall, and F1-Score.

	TP	TN	FP	FN	Accuracy	Precision	Recall	F1 Score
SVM	614	576	38	6	0.964	0.942	0.990	0.965
KNN	601	572	42	19	0.951	0.935	0.969	0.952
LogR	602	583	31	18	0.960	0.951	0.971	0.961
DL	3027	3077	6	56	0.990	0.998	0.982	0.990

Figure 9. Results of Applying three ML models and DL.

Tables 10–13 respectively reveal a graphical comparison between these values for the four models, while Figure 14 shows the shape of the scattering matrix generated from the learning curve code of the deep learning model to prove its effectiveness.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

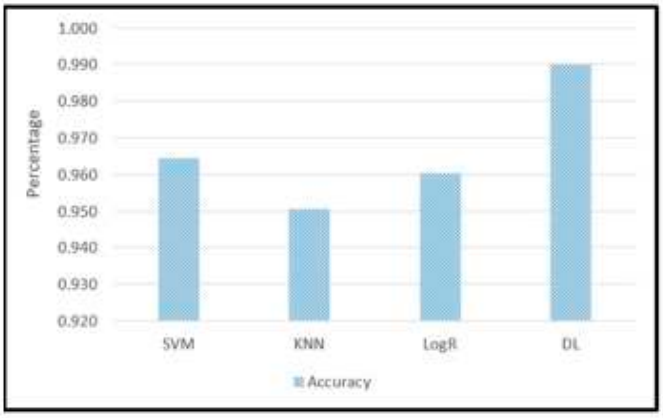

Figure 10. Accuracy result of SVM, KNN, Log R, and DL

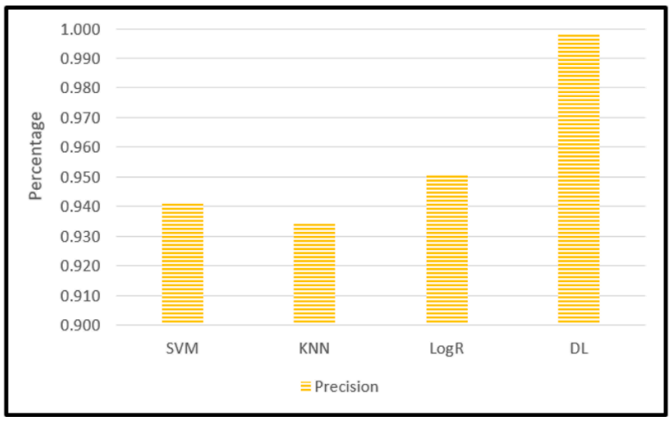

Figure 11. Precision result for SVM, KNN, Log R, and DL.

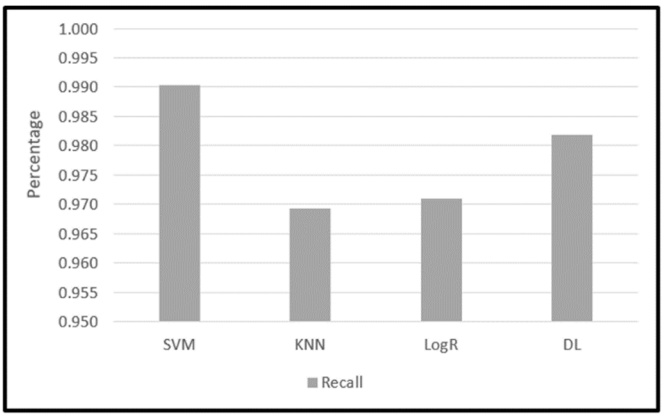

Figure 12. Recall result for SVM, KNN, Log R, and DL.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 26 September 2023 doi:10.20944/preprints202309.1742.v1

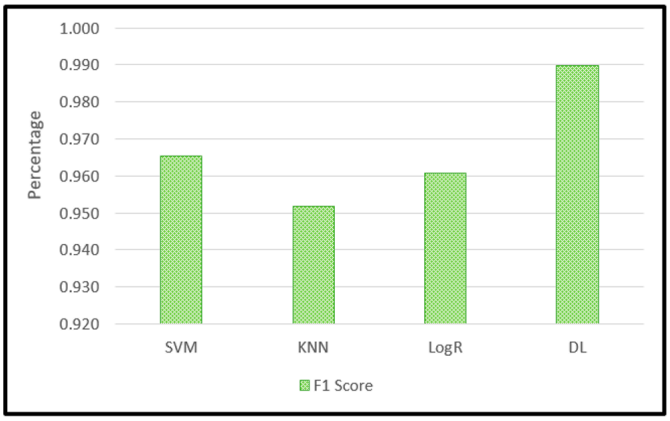

Figure 13. F1 Score result for SVM, KNN, Log R, and DL.

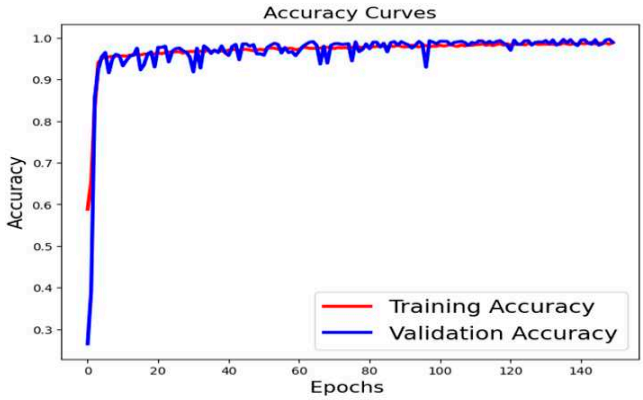

Figure 14. matching between training and validation accuracy**.**

Figure 14 reveals how exactly fit between validation accuracy and training accuracy results. While, Figure 15 depicts 3 machine learning models outcome comparing with deep learning model outcome in terms of accuracy, precision, Recall, and F1 Score outcomes.

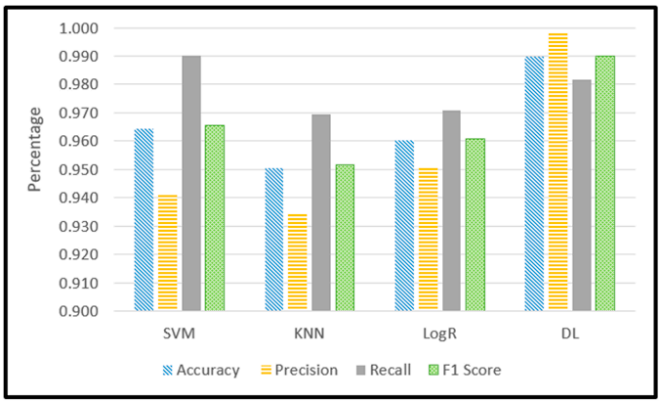

Figure 15. displays comparing among the four models.

8. Discussion and future trends

Based on all above, we note that all the previous solutions that have been negotiated and have spoken about the integration of the (Internet of things, machine learning, and Blockchain) suffer from the following negatives:

1. Depending on the Blockchain as an absolute solution to the issue of data security and privacy in the Internet of Things applications, which is inaccurate as the Blockchain may suit some

cases. Still, it may not help protect privacy in some applications and may be unsuitable for delay-sensitive real-time applications.

2. There is no genuine interest or special care in the privacy issue; some ignore it completely, and others consider it an element of security, which is not valid.
3. The solutions that employed machine learning in the same protection technology. I used it only to detect security threats and not privacy, such as sequences or intrusion, without concern for privacy issues, such as identity detection or the threat of tracking or profiling.
4. There are no independent solutions to the privacy problem (special protection techniques) or security solutions even commensurate with delay-sensitive or centralized applications.
5. Previous research (especially the one that discussed the issue of security as the main thing) was not concerned with the issue of testing possible attacks on data, whether security attacks or privacy attacks.

In the next research, we will seek to solve these previous problems and provide a more comprehensive solution so that the Machine Learning algorithm plays a more significant role in analyzing and detecting privacy and security threats, not just security threats. The solution also will provide a proposed solution to the security tripartite (CIA) problems and also the solution to the privacy threefold (Identification, Tracking, Profiling (ITP)) problems. In addition, the proposed solution also reports on the most severe attacks on privacy and data security. Finally, the proposed solution will provide different protection techniques suitable for the application of the Internet of Things system. Blockchain is one of its branches and not the only solution in it, where other privacy protection solutions will also be proposed. Moreover, the proposed resolution takes into account the performance issue by employing the fog structure within the proposed framework.

9. Conclusion

In this research, we have investigated security threats in IoT environment using Deep Learning algorithms and blockchain technology. We have focused on security requirements which are CIA, (Confidentiality, Integrity, and Availability). We have used decoding, hashing and fog computing with Cloud hierarchy respectively for each of the CIA associating machine learning, Deep learning and blockchain to enhance security level in IoT systems. We consider difference of value and difference of time as symptom of attack. So, we employed the two values in the dataset of implementation and testing. Our proposed classification and detection algorithm achieved more accuracy exceed 99% with DL model. Moreover, our framework has noticed that there is a significant difference will detect certain threat and determine which kind of CIA threats and notify sensor or device to stop it. Afterward, the hybrid framework will provide certain protection techniques based on what type of attacks were, in addition the proposed algorithm will work on detecting the privacy threats also.

References

1. Dedeoglu, V., Jurdak, R., Putra, G. D., Dorri, A., & Kanhere, S. S. (2019, November). A trust architecture for blockchain in IoT. In Proceedings of the 16th EAI international conference on mobile and ubiquitous systems: computing, networking and services (pp. 190-199).Tomar, P., Singh, S. K., Kanga, S., Meraj, G., Kranjčić, N., Đurin, B. and Pattanaik, A. [2021], 'Gis-based urban flood risk assessment and management—a case study of delhi national capital territory (nct), india', Sustainability 13(22), 12850.
2. Bao, Z., Shi, W., He, D., & Chood, K. K. R. (2018). IoTChain: A three-tier blockchain-based IoT security architecture. arXiv preprint arXiv:1806.02008.
3. Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P., & Aski, V. J. (2020). Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects. International Journal of Communication Systems, 33(12), e4443.
4. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal, 4(5), 1125-1142.
5. Kearney, P. (2020). Iot security: Experience is an expensive teacher. The Internet of Things: From Data to Insight, 107-120.
6. Jurcut, A. D., Ranaweera, P., & Xu, L. (2020). Introduction to IoT security. IoT security: advances in authentication, 27-64.

7. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. Journal of Network and Computer Applications, 88, 10-28.
8. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.
9. Pulkkis, G., Karlsson, J., & Westerlund, M. (2018). Blockchain-Based Security Solutions for IoT Systems. Internet of Things A to Z: Technologies and Applications, 255-274.
10. Khan, I., Belqasmi, F., Glitho, R., Crespi, N., Morrow, M., & Polakos, P. (2015). Wireless sensor network virtualization: A survey. IEEE Communications Surveys & Tutorials, 18(1), 553-576.
11. Aghazadeh, H., Germi, M. B., Khiav, B. E., & Ghadimi, N. (2015). Robust placement and tuning of UPFC via a new multiobjective scheme-based fuzzy theory. Complexity, 21(1), 126-137.
12. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal, 4(5), 1125-1142.
13. Modieginyane, K. M., Letswamotse, B. B., Malekian, R., & Abu-Mahfouz, A. M. (2018). Software defined wireless sensor networks application opportunities for efficient network management: A survey. Computers & Electrical Engineering, 66, 274-287.
14. Aman, M. N., Chua, K. C., & Sikdar, B. (2017). Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 4(5), 1327-1340.
15. Qu, C., Tao, M., Zhang, J., Hong, X., & Yuan, R. (2018). Blockchain based credibility verification method for IoT entities. Security and Communication Networks, 2018.
16. Jesus, E. F., Chicarino, V. R., De Albuquerque, C. V., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure internet of things and the stalker attack. Security and communication networks, 2018.
17. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. Sensors, 18(8), 2575.
18. Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot blockchain platform for sensing data integrity. sensors, 19(10), 2228.
19. Maroufi, M., Abdolee, R., & Tazekand, B. M. (2019). On the convergence of blockchain and internet of things (iot) technologies. arXiv preprint arXiv:1904.01936.
20. Choi, B. G., Jeong, E., & Kim, S. W. (2019). Multiple security certification system between blockchain based terminal and internet of things device: Implication for open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 5(4), 87.
21. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., & Zhang, Y. (2019). Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE network, 33(3), 10-17.
22. Aman, M. N., Sikdar, B., Chua, K. C., & Ali, A. (2018). Low power data integrity in IoT systems. IEEE Internet of Things Journal, 5(4), 3102-3113.
23. Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016, December). A denial of service attack method for an iot system. In 2016 8th international conference on Information Technology in Medicine and Education (ITME) (pp. 360-364). IEEE.
24. Yamin, M., Alsaawy, Y., B. Alkhodre, A., & Abi Sen, A. A. (2019). An innovative method for preserving privacy in Internet of Things. Sensors, 19(15), 3355.
25. Nguyen, T. A., Min, D., & Choi, E. (2020). A hierarchical modeling and analysis framework for availability and security quantification of IoT infrastructures. Electronics, 9(1), 155.
26. Singh, R., Tanwar, S., & Sharma, T. P. (2020). Utilization of blockchain for mitigating the distributed denial of service attacks. Security and Privacy, 3(3), e96.
27. Syed, N. F., Baig, Z., Ibrahim, A., & Valli, C. (2020). Denial of service attack detection through machine learning for the IoT. Journal of Information and Telecommunication, 4(4), 482-503.
28. Wu, J., Wang, C., Yu, Y., Song, T., & Hu, J. (2020). Sequential fusion to defend against sensing data falsification attack for cognitive Internet of Things. ETRI Journal, 42(6), 976-986.
29. Al-Turjman, F., & Alturjman, S. (2018). Confidential smart-sensing framework in the IoT era. The Journal of Supercomputing, 74(10), 5187-5198.
30. Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022). A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications, 16(5), 421-432.
31. Sadeghi-Niaraki, A. (2023). Internet of Thing (IoT) review of review: Bibliometric overview since its foundation. Future Generation Computer Systems
32. Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. Information, 12(2), 87.
33. Bahbouh, N. M., Compte, S. S., Valdes, J. V., & Sen, A. A. A. (2023). An empirical investigation into the altering health perspectives in the internet of health things. International Journal of Information Technology, 15(1), 67-77.

 doi:10.20944/preprints202309.1742.v1

34. Yamin, M., Basahel, A. M., & Abi Sen, A. A. (2018). Managing crowds with wireless and mobile technologies. Wireless Communications and Mobile Computing, 2018.
35. Marchi, G., Mulloni, V., Hammad Ali, O., Lorenzelli, L., & Donelli, M. (2021). Improving the sensitivity of chipless RFID sensors: The case of a low-humidity sensor. Electronics, 10(22), 2861.
36. Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10, 189-200.
37. Mololoth, V. K., Saguna, S., & Åhlund, C. (2023). Blockchain and machine° learning for future smart grids: A review. Energies, 16(1), 528.
38. Yu, F., Rao, W., Liu, C., Wang, J., & Zhou, L. (2022). Architecture, Integrated Gateway Design, And Performance Evaluation for High Concurrency Access of Power Internet of Things. Mobile Information Systems, 2022.
39. Kaur, B., Dadkhah, S., Shoeleh, F., Neto, E. C. P., Xiong, P., Iqbal, S., ... & Ghorbani, A. A. (2023). Internet of things (IoT) security dataset evolution: Challenges and future directions. Internet of Things, 100780.
40. Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. International Journal of Information Technology, 13, 829-837.
41. Donta, P. K., Srirama, S. N., Amgoth, T., & Annavarapu, C. S. R. (2022). Survey on recent advances in IoT application layer protocols and machine learning scope for research directions. Digital Communications and Networks, 8(5), 727-744.
42. Nath, R., & Nath, H. V. (2022). Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. Computers and Electrical Engineering, 100, 107997.
43. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. Ieee Access, 8, 165130-165150.