Journal of
*Sensor and Actuator Networks*

MDPI

*Article*

# A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems

**Geetanjali Rathee [1], Chaker Abdelaziz Kerrache [2] and Mohamed Amine Ferrag [3,*]**

[1] Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi 110078, India
[2] Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat 03000, Algeria
[3] Department of Computer Science, Guelma University, Guelma 24000, Algeria
* Correspondence: ferrag.mohamedamine@univ-guelma.dz

**Abstract:** The industrial internet of things (IIoT) is considered a new paradigm in the era of wireless communication for performing automatic communication in the network. However, automatic computation and data recognition may invite several security and privacy threats into the system during the sharing of information. There exist several intrusion detection systems (IDS) that have been proposed by several researchers. However, none of them is able to maintain accuracy while identifying the threats and give a high false-positive rate in the network. Further, the existing IDS are not able to recognize the new patterns or anomalies in the network. Therefore, it is necessary to propose a new IDS. The aim of this paper is to propose an IDS using the Viterbi algorithm, indirect trust, and blockchain mechanism for IIoT to ensure the required security levels. The Viterbi algorithm and indirect trust mechanism are used to measure the probability of malicious activities occurring in the network while generating, recording, and shipping products in an IIoT environment. Further, the transparency of the system is maintained by integrating blockchain mechanisms with Viterbi and indirect methods. The proposed framework is validated and analyzed against various security measures by comparing it with the existing approaches.

**Keywords:** Industrial IoT; blockchain network; Viterbi algorithm; trust evaluation; Secure IIoT system



**Citation:** Rathee, G.; Kerrache, C.A.; Ferrag, M.A. A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems. *J. Sens. Actuator Netw.* **2022**, *11*, 71. https://doi.org/10.3390/jsan11040071

Academic Editors: Lei Shu and Houbing Song

Received: 6 September 2022
Accepted: 21 October 2022
Published: 27 October 2022



## 1. Introduction

The expeditious evolution in wireless communication has provided several solutions to day-to-day life issues ranging from electronic watches and fitness bands for monitoring health to data storing and management. The demand and roles of wireless devices are increasing day by day. The integration of intelligent systems with wireless devices has been further increased by the better utilization and efficiency of tasks occurring via networks [1,2]. The industrial internet of things (IIoT) is defined as a ubiquitous network where a number of devices are connected to the internet for performing various tasks such as computing, decision-making, data gathering, etc. [3]. The IIoT is considered as a paradigm where interconnected smart devices are increasing year by year to fully take over the computation and communication processes from the environment. The advances of the internet have fueled the growth of the industrial internet of things, where new technologies such as 5G focus on improving the connectivity of smart devices in various industrial sectors such as agriculture, manufacturing, gas and oil, and healthcare [4–6]. IIoT systems gather several types of information regarding manufacturing, shipping, and recording and storing of raw and finished products. These systems also maintain information containing traffic records or data generated during industrial processes. The data generated from various smart devices further plays a very crucial role in industrial sectors [7,8].

In order to effectively utilize industrial information, better methods of data collection, management, and transmission are proposed to enhance its potential value. Further, there

exist various traditional ways to connect to the internet, including TCP/IP. However, LAN and WAN make the network susceptible to various security and privacy threats that might jeopardize the IIoT system [9,10]. On the one hand, where IIoT platforms offer varied services and are diverse in gathering, manufacturing, and shipping provisions. On the other hand, IIoT devices and infrastructure can also be susceptible to several critical threats. The data collection and recording of manufacturing data may lead to various types of networking threats, such as denial of service attack thus affecting accuracy, authentication, etc.

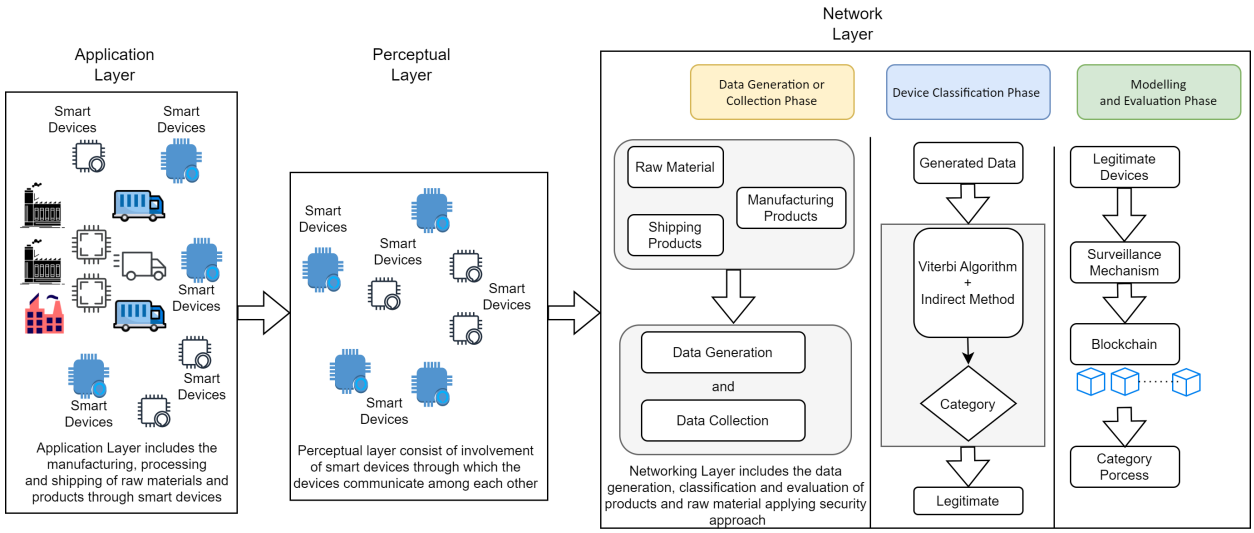


**Figure 1.** Typical Architecture of an IIoT System.

### *1.1. Motivation and Objective*

Figure 1 presents the layered diagram of an IIoT system consisting of the application layer, perceptual layer, and network layer based on data flow. The application layer consists of all the physical devices through which manufacturing, shipping, and processing are performed. The second layer is the perceptual layer, in which the communication among devices is performed automatically and intelligently. Finally, the network layer consists of various sub-phases, i.e., data generation and collection, device classification, and modeling and evaluation. Data generation and collection is the first phase, where the information generated from the environment is captured and gathered by multiple smart sensors in the network. The huge amount of generated data is further processed to get the actual information which, in the context of industries, can be manufacturing and shipping information. Now, in the second phase, where devices collect information from the environment, the network can be compromised by various intruders through malicious devices. The device classification based on their generated and collected information can either be legitimate or altered. In order to categorize the devices in our proposed approach, we have used two secure schemes, i.e., the Viterbi algorithm and the indirect method. Finally, in the third phase, the categorized devices are further traced continuously through a blockchain mechanism in the network. All the phases have their own responsibility and can be identified at the same level in the network.

Each layer is susceptible to several types of threats and intrusions that may occur within IIoT. Some general intrusions and attacks in an IIoT environment include data corruption, denial of service, jamming, and authentication attacks. In order to counter these malicious threats, it is further needed to guarantee the security and privacy of the information generated, recorded, and stored. In order to maintain the security and communication process among intelligent devices, a number of organizations are implementing an intrusion detection system (IDS) that can be configured at any layer of the system. The IDS plays a significant role by guaranteeing security, integrity, and privacy of data generated and transmitted via various networks.

An IDS can detect, react, protect, and report any type of malicious activity or attack. Traditional IDSs are broadly categorized into several types, such as signature-based, anomaly-based, or both (signature and anomaly-based). Anomaly-based IDS systems are implemented by observing various abnormal patterns, while signature-based IDS are designed by using traditional threat signatures in their database. Existing IDSs are not able to maintain accuracy while identifying the threat, and they provide a high false-positive rate in the network. However, existing IDSs are not able to recognize new patterns or anomalies in the network. In order to enhance the performance of existing IDSs, researchers have designed the trust rate, more particularly, an indirect type of trust computation process and blockchain mechanism for IDS.

Trust is considered one of the significant factors of the device for recognizing the legitimacy and behavior of the network. The proposed mechanism provides an intrusion detection system that includes a Vertibi algorithm and indirect trust computation for enhancing security and privacy in the network [11,12]. In addition, indirect trust and the Vertibi algorithm are also used to make an independent decision while transmitting the information in the network. A blockchain mechanism is also integrated with the IDS to maintain transparency in the system [13,14].

### *1.2. Contribution*

Below, we briefly explain the contributions of our study in four points:

- First, we propose a Viterbi algorithm to generate the fitness score and accuracy of the decision-making process by each communicating node in the network.
- Secondly, an indirect trust computation method is used to analyze the legitimacy and malicious behavior of each node.
- Lastly, a blockchain mechanism is integrated with the Viterbi algorithm and indirect trust method for maintaining transparency and security in the IIoT system.
- A thorough comparison is conducted between the existing and proposed mechanism for validating and verifying the out-performance of the system against various security measures. The simulated results demonstrate the worthy improvement in the IIoT performance.

The overall structure of the paper is discussed as follows. Section 1 discusses the motivation and significance of proposing an intrusion detection system using Viterbi algorithm and a blockchain mechanism. Section 2 deliberates upon the related work that illustrates several approaches and methods proposed by earlier scientists and researchers for ensuring a secure and trusted communication mechanism in various IoT-based applications, specifically in IIoT. Further, Section 3 proposes a secure and trusted mechanism by explaining the Viterbi algorithm, indirect trust, and blockchain technology in detail. The proposed mechanism is an intrusion detection system integrated with the Viterbi algorithm for identifying the legitimacy of each communicating device based on some probability values in the network. The proposed framework further uses blockchain technology, where a block is maintained for each legitimate node in the network for continuous surveillance and transparency of data transmission in the network. Furthermore, Section 4 illustrates the experimentation and validation of the proposed framework by considering several security metrics, such as false positive rate, false negative rate, accuracy, and response time, in comparison to existing approaches. Finally, Section 5 outlines the conclusion along with some future directions of the paper.

## 2. Related Work

This section deliberates the number of security mechanisms [15–18] proposed by various researchers and scientists. Yao et al. [19] surveyed the state of the threat literature regarding identification systems and methods of intrusion detection. The authors have further proposed a hybrid intrusion detection architecture by introducing a machine learning-aided method. The authors have validated the proposed mechanism by showing its out-performance in the range of various benchmarks. Alsaedi et al. [20] addressed

the issues of intrusion and threat possibilities in IIoT networks and have proposed a data-driven IIoT dataset by identifying the labeling features of various attack classes using multi-classification. The proposed dataset, named telemetry data, is gathered from a realistic medium-scale network. The authors have also described the various characteristics and benefits by determining various attacks and normal events from heterogeneous sources. The proposed mechanism is then evaluated using deep learning and machine learning mechanisms in both multi-class and binary-class classification issues for intrusion purposes.

**Table 1.** Related Work Discussion.

| Author Name | Description | Limitation |
| --- | --- | --- |
| Yao et al. [19] | Authors have further proposed a hybrid intrusion detection architecture by introducing a machine learning-aided method. | The authors have used machine learning techniques that may further increase the computational steps in the network. |
| Kasongo [21] | The authors have proposed an IDS genetic algorithm that further includes extra trees, naïve Bayes, linear regression, decision tree, and RF. | The integration of multiple algorithms increased the complexity and computation in the network. |
| Basset et al. [22] | The authors have proposed a forensics-based deep learning mechanism for identifying intrusions in industrial traffics. | The deep learning mechanism may further involve multiple layers to identify the legitimacy of a device, which may further increase the delay in the network. |
| Alruwaili [23] | The authors have proposed and investigated cybersecurity issues by identifying the prevention and intrusion detection gaps in the field of IIoT. | The authors have not identified the threats specifically related to industrial sectors. |
| Gyamfi and Jurcut [24] | The authors have proposed a lightweight intrusion detection system based on online support vector data description using an adaptive sequential learning machine. | The proposed mechanism increased the communicational overhead in the network. |
| Yazdinejad et al. [25] | The authors have proposed a federated learning mechanism to build a framework for automatically hunting the threats in blockchain-based industrial networks. | The proposed framework may further increase the storage and computational overhead while categorizing or identifying the legitimate devices in the network |

Kasongo [21] has proposed an IDS genetic algorithm that further includes the extra trees, naïve Bayes, linear regression, decision tree, and RF. The proposed mechanism is used to access the robustness and effectiveness of the proposed framework by demonstrating the accuracy of the modeling process. The proposed mechanism is further validated by considering various features as compared to existing detection systems. Basset et al. [22] projected forensics-based deep learning schemes for identifying intrusions in industrial traffic. The projected model is used to identify the local and global multi-head attention to capture the traffic sequence in IIoT. The authors have also addressed the scalability issue by proposing a fog computing environment using aggregating classification outputs. The proposed approach is verified against several security parameters, such as robustness, by presenting the centralized IDS environment. Alruwaili [23] has proposed and investigated cybersecurity issues by identifying the prevention and intrusion detection gaps in the field of IIoT. The authors have then compared the various mechanisms to prevent, detect, and protect smart industrial systems against threats, vulnerabilities, and attacks. Further, the authors have expanded the issue by utilizing 5G, AI, and blockchain technology to offer various future challenges. Gyamfi and Jurcut [24] have proposed a lightweight intrusion detection mechanism based on an online support vector data description using an adaptive sequential learning machine. The proposed model is saturated by applying the data filtering convergence rate. The proposed mechanism is evaluated using an experimental and self-generated dataset. The proposed model performed and detected effectively in a realistic IIoT environment.

Yazdinejad et al. [25] projected a federated learning approach to build a framework for automatically hunting the threats in blockchain-based industrial networks. In order to automatically detect the threats, the authors have used a cluster architecture for identifying

anomalies using various machine learning schemes in a federated environment. The authors have claimed this approach as the first federated framework for identifying anomalies by preserving the behavior in IIoT networks. Rathee et al. [26] proposed a blockchain-based, secure industrial trust evaluation mechanism to analyze voting using weights for approaching the final decision authorization. The designed voting scheme was effective with a trust evaluation system for a higher probability of malicious IIoT detection system.

Further, [27–30] have proposed some blockchain-based intrusion detection mechanisms for further ensuring secure communication and transmission of information in the network. Though various security schemes have been proposed by the scientists, however, the proposal of an efficient, secure mechanism for IIoT by reducing the response time and improving the accuracy in the network is needed.

Table 1 summarises the main existing works.

## 3. Proposed Approach

Figure 2 illustrates the IDS of the proposed approach, having a number of inputs that are separated into three different phases, namely, the data collection or generation phase, device classification phase, and modeling and evaluation phase. In the data collection and generation phase, the dataset is loaded for validation and testing. Further, the classification phase is the one where the devices are categorized into two distinct categories, i.e., legitimate and malicious, depending upon the information process and transmission by the devices in the IIoT. An IDS, including Viterbi and indirect methods, is also introduced in the classification phase of the system to categorize and recognize the legitimacy of every communicating device in the network. In addition, the third phase includes the blockchain mechanism, where the devices are finally surveyed and validated on a regular basis in the IIoT system. The building blocks of the projected mechanism are illustrated in a more detailed way in the succeeding subsections.

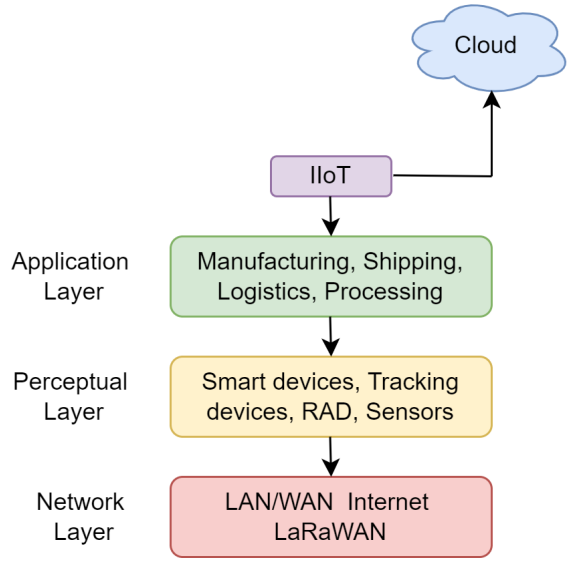


**Figure 2.** Proposed IDS Mechanism for IIoT.

### *3.1. Data Generation and Collection Phase*

The most important aspect of using the data collection and generation phase to process the request from various stages of industry such as the collection of raw material with its proper counting, the record of manufacturing products, and the storing and shipping process of products via intelligent devices are actually analyzed and processed by smart devices before actually checking their validity and legitimacy in the network. The min-max scaling process is applied for data collection and generation of information in the IIoT system as follows.

$$P = \frac{(x-y)P_n - min(P_n)}{max(P_n) - min(P_n)} \quad (1)$$

### 3.2. Classification Phase

The generated records by smart devices are now actually processed via IDS, including Viterbi and an indirect method, for further analyzing their behavior and categorizing them into various categories, such as malicious and legitimate. In the first step, we used the Viterbi algorithm to identify the probability of altered devices based on their internal activities and emissions. The depicted steps illustrate the identification process of various malevolent activities of transmitting devices in the network. Let PRt(n) illustrate the highest probability of a device in a particular state i having o observations and l sequence length, the probability rate can be further identified as below:

$$PR_t(i) = maxPR(\phi(1), \phi(2)....\phi(t-1); \mu(1), \mu(2)....\mu(t) | \lambda(t) = \lambda_i \quad (2)$$

### 3.3. Viterbi Method

Table 2 represents the abbreviations or notations that are used while defining the Viterbi algorithm.

**Table 2.** Notations of Viterbi Algorithm.

| Symbol | Definition |
|---|---|
| $PR_t(n)$ | Probability rate of device from i to j state having 'l' sequence of input |
| $\alpha_{Ri}$ | Initial probability rate of state i |
| $bR_i(\lambda(t))$ | Probability rate output of state i |
| $\alpha_{Rij}$ | Transition from state i to j |

The number of steps required to compute the probability rate of each communicating node using Viterbi algorithm is discussed as follows:

**Input Value:** (1) 'n' Number of IoT devices, (2) sequence of inputs

**Output:** Device is categorized as legitimate of malicious

**Step 1.1:** Initialization of probability rate and matrix as:

$$PR_t(n) = \alpha_{R_i BR_i}(\lambda(t)) \quad (3)$$

$$\alpha_{R_i(t)} = 0 \quad (4)$$

**Step 1.2:** Recursion by performing the updates as:

$$PR_t(i) = max[PR_{t-1}\alpha_{R_{ij}}]bR_j(\phi(t)) \quad (5)$$

**Step 1.3:** Recursion is terminated as:

$$R^* = max - i[PR_t(i)] \quad (6)$$

$$R^* = argmax - i[PR_t(i)] \quad (7)$$

**Step 1.4:** The final state is identified using backtracking as:

$$R_t^* = \alpha_{R_{t-1}(R_t^*+1)} \quad (8)$$

**Indirect Trust()**

**Step 2.1:** The classified devices are identified as c1, c2,...cn according to their trust values by defining the root mean square function.

$$ITV_{cnj}(rms) = \frac{\sqrt{\sum_{x=1} nITV_{cxj}^2}}{n} \tag{9}$$

where $i$ and $j$ are defined as various states according to their trust rate, and x is considered as the device.

**Step 2.2:** In addition, the understanding degree to know the best communicating device having the highest trust rate is defined as:

$$U_d = \frac{n}{N} e^{-\rho(t-t_0)} \tag{10}$$

where $\rho$ is the coefficient to define the starting point in time.

**Step 2.3:** Further, the conflict among communicating devices having the same trust rate can be defined as:

$$C_d = \sum_{n!=m} \frac{ITV_{cn} - ITV_{cm}}{n} \tag{11}$$

where, the larger the $C_d$, the more $C$ recommendations deviate from their behavior.

**Step 2.4:** Finally, the similarity rate among subject and recommender rates are considered as:

$$ITV_{ij} = \frac{1}{m} \sum_{n=1} mITV_{ica} \times ITV_{caj} \tag{12}$$

Finally, a blockchain network is maintained to maintain transparency among each communicating device in the IIoT environment.

**Blockchain Network ()**

Block $d_1$, block $d_2$... block $d_n$

Where block d contains the hash, old hash, and the actual information (raw product count, manufacturing product count, shipping count) in the network.

The proposed mechanism provided an efficient and secure communicating IDS framework by integrating Viterbi, indirect, and blockchain mechanisms in an IIoT environment. The Viterbi algorithm is used to calculate the probability rate of each communicating device based on their activities and sequences. In addition, the probability rate computation can be further increased by using indirect trust computation by categorizing each device. Finally, continuous surveillance and transparency are further maintained using the blockchain mechanism. The proposed system's efficiency and validity are further analyzed by simulating using MATLAB. The validation and verification process over various security measures are explained in detail in the next section.

## 4. Performance Analysis

Figure 2 explains the process that can be followed while applying the proposed scenario in IIoT applications. At present, we have considered some random set of devices that collect information and records by generating synthesized data having product names and counts in order to check the working of the projected framework. The simulation of the proposed framework is implemented using MATLAB 2019b on windows 10 OS to verify its performance. In the simulation process, the number of B-IIoT devices is considered as 50 with a time slot of 50. The proposed approach's Viterbi and indirect schemes are verified over a synthesized dataset having 50 IoT devices that are further categorized as legitimate or altered. The malicious behavior of any device is identified by recognizing its internal behavior and activity in the network. The number of communicating devices is intentionally converted from legitimate to malicious in order to validate the proposed scenario where for every 10 devices, 5% of the devices are altered from legitimate to malicious. In addition,

the reliability, transparency, and optimum behavior of each device are analyzed over 3000 epochs with 9.6732, 4.056, and 4.54 s time using the Viterbi algorithm.

### 4.1. Baseline Mechanisms

The proposed framework is analyzed against two baseline methods from Yazdinejad et al. [25] and Rathee et al. [26] in terms of several security parameters, such as false positive rate, false negative rate, accuracy, and response time. The baseline methods are further added to the proposed framework in order to understand the proposed scheme used to improve security. Further, the proposed framework is analyzed against Yazdinejad et al. [25] and Rathee et al. [26] to show its performance. The proposed framework is simulated over two various existing approaches in order to measure the validity of IDS in IIoT systems. Yazdinejad et al. [25] (as Baseline Approach 1 (BA1)) proposed a federated learning mechanism to build a framework for automatically hunting the threats in blockchain-based industrial networks. In order to automatically detect the threats, the authors used a cluster architecture for identifying the anomalies using various machine learning schemes in a federated environment. The authors have claimed the proposed as the first federated framework for identifying the anomalies by preserving the behavior in IIoT networks. Rathee et al. [26] (as Baseline Approach 2 (BA2)) proposed a blockchain-based secured industrial trust evaluation mechanism to analyze the voting through weights for their final decision authorization. The designed voting scheme was used with a trust evaluation for a higher probability of the detection of a malicious system. The simulated results are demonstrated by the trust evaluation process using correct authorization. The proposed mechanism is validated against both approaches, further showing the benefit of introducing transparency using the blockchain in the IIoT systems.

### 4.2. Measuring Parameters

False positive: The number of devices recognized as ideal or legitimate while malicious. The network of devices labeled as intruders while they are actually malicious False negative: The number of devices recognized as malevolent while legitimate. The network of devices is labeled as malicious while they are actually ideal. System accuracy: The network is accurately able to recognize all processes, such as data collection, manufacturing records, and shipping product information, via intelligent devices. Response time: The amount of time needed by the system to provide the requested data to the device.

### 4.3. Evaluation

After the setup of the simulation process, the results are analyzed against all the approaches in the network. The projected mechanism is compared to Yazdinejad et al. [25] and Rathee et al. [26], and various security metrics are analyzed. The communication process is performed over web requests generated by intruders over virtual machines. Depending upon the generated requests and device category, such as legitimate or malicious, the proposed mechanism is verified in IIoT systems. Further, the number of input metrics of the intruder's resource is depicted in Table 3.

**Table 3.** Result analysis.

| Type | % of Threat Request | Phases of Security | Source Name |
|---|---|---|---|
| Ideal | 0 | 0 | 25 |
| Malevolent | 15% | 2, 3 | 10 |
| Prone to threat | 20% | 1, 4, 5 | 15 |

The validation of the proposed phenomenon is again measured over two significant metrics, such as false negative and false positive. False positive can be termed as the case where communicating devices are recognized as legitimate. However, they are actually altered by the intruders to act as malevolent. On the contrary, false negatives occur when

devices are recognized as malicious, despite the fact that they are legitimate. Both the performances are recognized for the baseline solution and the proposed scheme to further the recognition of accuracy by the system.

Figure 3 illustrates the false positives scenario where the proposed scheme outperforms in comparison to the baseline method because of their indirect method trust calculation that reflects the legitimate behavior of each transmitting device. The devices having higher trust rates are detected as legitimate. However, devices having lesser trust values are recognized as malevolent because they can be easily traced with the proposed method.

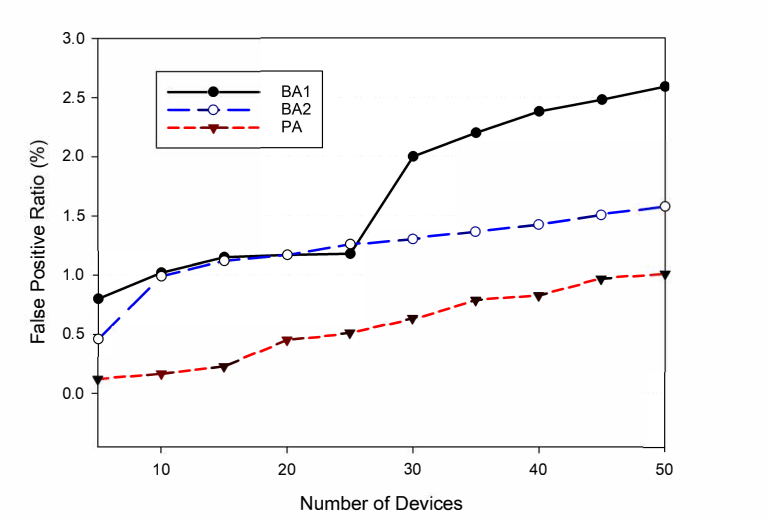


**Figure 3.** False positive ratio of the proposed approach compared to the baseline approaches.

In addition, Figure 4 illustrates the false negatives scenario where the legitimacy of each transmitting device can be easily recognized with their trusted values and reinforcement learning. The recognition of false negative counts is better in our proposed method as compared to the baseline methods.

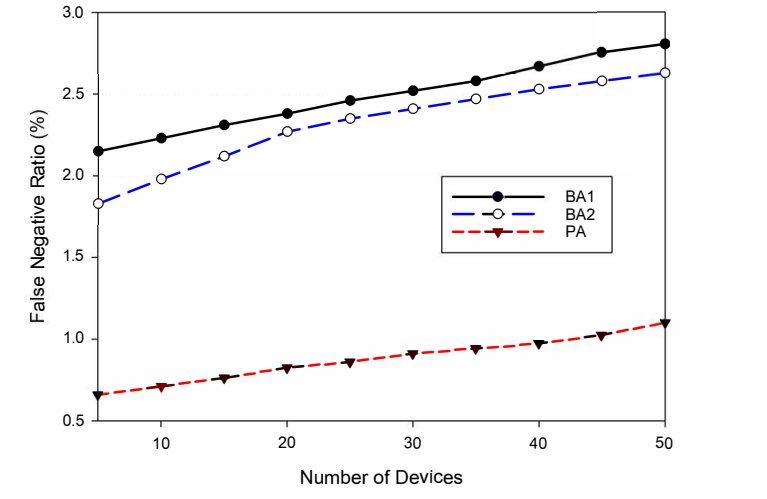


**Figure 4.** False negative ratio of the proposed approach compared to the baseline approaches.

In addition, Figure 5 determines the accuracy of the proposed mechanism; how accurately the system is able to identify the security of communicating devices during information generation, maintaining, and the shipping process. The proposed mechanism outperforms the existing scenarios because of the instruction of the blockchain network in the system that continuously surveils the environment.

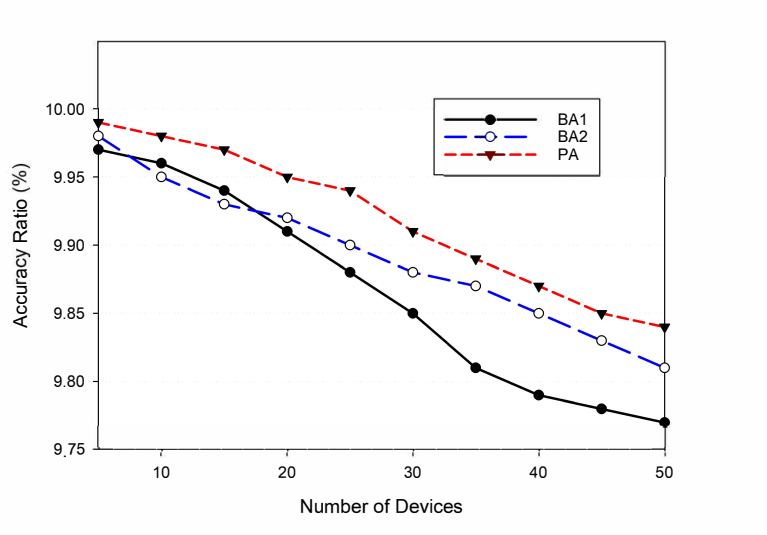


**Figure 5.** Proposed approach's accuracy compared to the baseline approaches.

Finally, Figure 6 presents the response time of the systems; the amount of time needed by the system to provide the requested information to the device. The response time of the proposed framework is much less compared to both existing systems.

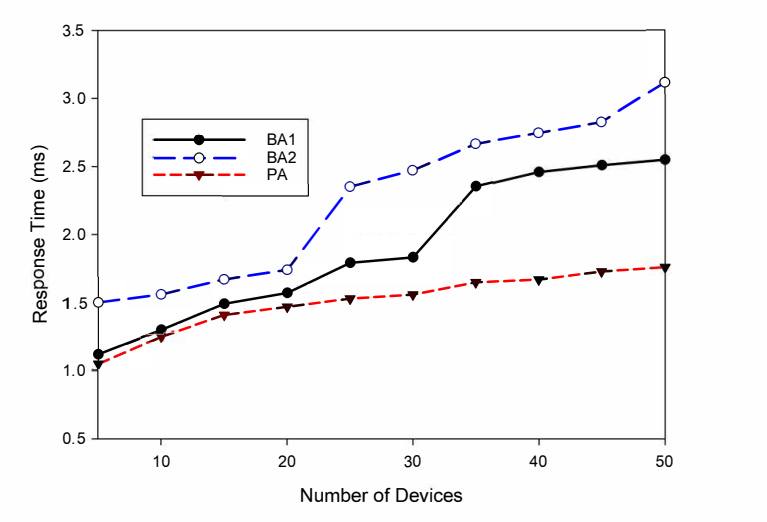


**Figure 6.** Proposed approach's response time compared to the baseline approaches.

## 5. Conclusions

This paper proposed a secure and transparent transmission mechanism in IIoT by introducing an efficient intrusion recognition system. The proposed mechanism used the Viterbi algorithm, indirect trust, and blockchain technology to ensure a secure network. The proposed system used the indirect and Viterbi algorithm to make an independent decision while transmitting information from the network. Further, a blockchain mechanism is integrated with the IDS to maintain transparency in the system. The Viterbi algorithm is used to measure the probability of malicious devices in the network. At the same time, the indirect trust is used to speed up the process of probability identification of malicious behavior of any device. The proposed mechanism is verified against several security parameters that show the increased performance of the system against various existing schemes. The collection of information from heterogeneous networks and the dynamic behavior of smart devices during mobility further plays a crucial role in identifying devices' legitimacy. Types of cyber threats and their corresponding IoT security solutions can be considered as the future scope of this manuscript.

**Author Contributions:** Conceptualization, G.R., C.A.K. and M.A.F.; methodology, C.A.K.; software, G.R.; validation, G.R., C.A.K. and M.A.F.; formal analysis, G.R., C.A.K. and M.A.F.; investigation, G.R. and C.A.K.; resources, G.R., C.A.K. and M.A.F.; data curation, G.R., C.A.K. and M.A.F.; writing—original draft preparation, G.R. and C.A.K; writing—review and editing, M.A.F.; visualization, G.R., C.A.K. and M.A.F.; supervision, M.A.F.; project administration, M.A.F.; funding acquisition, M.A.F. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** All implementation details, sources, and data will be delivered upon requesting the corresponding author Dr Mohamed Amine Ferrag.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Wilamowski, B.M.; Irwin, J.D. (Eds.). *Intelligent Systems*; CRC Press: Boca Raton, FL, USA, 2018
2. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
3. Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Nayak, J. Industrial Internet of Things and its applications in industry 4.0: State of the art. *Comput. Commun.* **2021**, *166*, 125–139. [CrossRef]
4. Tian, S.; Yang, W.; Le Grange, J.M.; Wang, P.; Huang, W.; Ye, Z. Smart healthcare: Making medical care more intelligent. *Glob. Health J.* **2019**, *3*, 62–65. [CrossRef]
5. Gollmann, D. Computer security. *Wiley Interdiscip. Rev. Comput. Stat.* **2010**, *2*, 544–554. [CrossRef]
6. Yang, H.; Bao, B.; Li, C.; Yao, Q.; Yu, A.; Zhang, J.; Ji, Y. Blockchain-enabled tripartite anonymous identification trusted service provisioning in industrial IoT. *IEEE Internet Things J.* **2021**, *9*, 2419–2431. [CrossRef]
7. Ceccarelli, A.; Cinque, M.; Esposito, C.; Foschini, L.; Giannelli, C.; Lollini, P. FUSION—Fog computing and blockchain for trusted industrial internet of things. *IEEE Trans. Eng. Manag.* **2020**, 1–15 . [CrossRef]
8. Yu, K.; Tan, L.; Aloqaily, M.; Yang, H.; Jararweh, Y. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7669–7678. [CrossRef]
9. Yang, Q.; Wang, H.; Wu, X.; Wang, T.; Zhang, S.; Liu, N. Secure Blockchain Platform for Industrial IoT with Trusted Computing Hardware. *IEEE Internet Things Mag.* **2021**, *4*, 86–92. [CrossRef]
10. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
11. Tan, S.F.; Samsudin, A. Recent Technologies, Security Countermeasure and Ongoing Challenges of Industrial Internet of Things (IIoT): A Survey. *Sensors* **2021**, *21*, 6647. [CrossRef] [PubMed]
12. Lou, H.L. Implementing the Viterbi algorithm. *IEEE Signal Process. Mag.* **1995**, *12*, 42–52. [CrossRef]
13. Su, B.; Du, C.; Huan, J. Trusted opportunistic routing based on node trust model. *IEEE Access* **2020**, *8*, 163077–163090. [CrossRef]
14. Fu, X.; Wang, H.; Shi, P. A survey of Blockchain consensus algorithms: Mechanism, design and applications. *Sci. China Inf. Sci.* 2021, *64*, 121101. [CrossRef]
15. Lin, Y.; Gao, Z.; Shi, W.; Wang, Q.; Li, H.; Wang, M.; Rui, L. A Novel Architecture Combining Oracle with Decentralized Learning for IIoT. *IEEE Internet Things J.* **2022**. [CrossRef]
16. Iqbal, S.; Noor, R.M.; Malik, A.W.; Rahman, A.U. Blockchain-enabled adaptive-learning-based resource-sharing framework for IIoT environment. *IEEE Internet Things J.* **2021**, *8*, 14746–14755. [CrossRef]
17. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain-based massive data dissemination handling in IIoT environment. *IEEE Netw.* **2020**, *35*, 318–325. [CrossRef]
18. Li, T.; Tian, Y.; Xiong, J.; Bhuiyan, M.Z. FVP-EOC: Fair, Verifiable and Privacy-Preserving Edge Outsourcing Computing in 5G-enabled IIoT. *IEEE Trans. Ind. Inform.* **2022**. [CrossRef]
19. Yao, H.; Gao, P.; Zhang, P.; Wang, J.; Jiang, C.; Lu, L. Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection. *IEEE Netw.* **2019**, *33*, 75–81. [CrossRef]
20. Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. *IEEE Access* **2020**, *8*, 165130–165150. [CrossRef]
21. Kasongo, S.M. An advanced intrusion detection system for IIoT based on GA and tree based algorithms. *IEEE Access* **2021**, *9*, 113199–113212. [CrossRef]
22. Abdel-Basset, M.; Chang, V.; Hawash, H.; Chakrabortty, R.K.; Ryan, M. Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment. *IEEE Trans. Ind. Inform.* **2020**, *17*, 7704–7715. [CrossRef]
23. Alruwaili, F.F. Intrusion Detection and Prevention in Industrial IoT: A Technological Survey. In *Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*; IEEE: New York, NY, USA, 2021; pp. 1–5.
24. Gyamfi, E.; Jurcut, A.D. Novel Online Network Intrusion Detection System for Industrial IoT based on OI-SVDD and AS-ELM. *IEEE Internet Things J.* **2022**. [CrossRef]

25. Yazdinejad, A.; Dehghantanha, A.; Parizi, R.M.; Hammoudeh, M.; Karimipour, H.; Srivastava, G. Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks. *arXiv* **2022**, arXiv:2204.09829.
26. Rathee, G.; Kerrache, C.A.; Lahby, M. TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT. *IEEE Trans. Ind. Inform.* **2022**, 1–8. [CrossRef]
27. Rathee, G.; Ahmad, F.; Hu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. *Inf. Process. Manag.* **2021**, *58*, 102526. [CrossRef]
28. Le, T.T.H.; Oktian, Y.E.; Kim, H. XGBoost for Imbalanced Multiclass Classification-Based Industrial Internet of Things Intrusion Detection Systems. *Sustainability* **2022**, *14*, 8707. [CrossRef]
29. Tharewal, S.; Ashfaque, M.W.; Banu, S.S.; Uma, P.; Hassen, S.M.; Shabaz, M. Intrusion detection system for industrial Internet of Things based on deep reinforcement learning. *Wirel. Commun. Mob. Comput.* **2022,** *2022*, 9023719. [CrossRef]
30. Mansour, R.F. Blockchain assisted clustering with Intrusion Detection System for Industrial Internet of Things environment. *Expert Syst. Appl.* **2022,** *207*, 117995. [CrossRef]