International Journal on Computational Modelling Applications
Vol. 02, Iss. 01, S. No. 002, pp. 15-27, March 2025
ISSN (Online): 3048-8516

Computation Intelligence Techniques for Security in IoT Devices

Sandeep Singh Sikarwar

Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, India
sandeepsikarwar@galgotiacollege.edu

How to cite this paper: Sandeep Singh Sikarwar, "Computation Intelligence Techniques for Security in IoT Devices", *International Journal on Computational Modelling Applications*, Vol. 02, Iss. 01, S. No. 002, pp. 15-27, March 2025.

Received: 13/01/2025
Revised: 02/02/2025
Accepted: 06/02/2025
Published: 10/02/2025

Abstract

This paper provides an overview of the context of security in Internet of Things (IoT) devices. It introduces the fundamentals of IoT definitions, and fifth generation (5G) networks and focuses on security in IoT devices. An introduction to computational intelligence techniques is also presented, including their evolution, use cases, significance, and standardization efforts, with examples. This paper presents a taxonomy of cyber threats targeting IoT devices and a review of several key works in every security category in IoT devices. It also explores the application of computational intelligence techniques to enhance the security of IoT devices. Providing a comprehensive overview of models or mechanisms such as machine learning (ML), deep learning (DL), fuzzy systems (FS), and evolutionary algorithms (EA). Their model role is to detect and mitigate security threats in the IoT system. The paper shows the successful application of computational intelligence in enhancing IoT security through case studies and practical examples. Next, this paper discusses new challenges and future research directions in IoT device security.

Keywords

Internet of Things, Fifth Generation (5G), Computational Intelligence Techniques (CIT), Security, Machine Learning, Deep Learning, Fuzzy Systems.

1. Introduction

The Internet of Things (IoT) refers to a network of interconnected physical devices that can communicate with each other; there is no need for human involvement, only use via the Internet. Such devices, which range from everyday household devices like refrigerators and heating and cooling systems to heavy industrial machinery, are embedded with sensors, software, and other technologies that allow them to gather and share data. The ultimate target of IoT is to create a more responsive, intelligent environment by automating and improving processes across various fields, such as healthcare, manufacturing, transportation, and home automation. The motivation for defining and understanding IoT lies in its transformative potential across multiple industries. As IoT devices increase rapidly, they allow real-time data collection and analysis. Leading to more efficient operations, improved customer experiences, and the creation of a new business model [1]. However, it rapidly increases the security issued in IoT. It introduces significant security challenges, as each connected device represents a potential cyber-attack entry point. Therefore, a comprehensive understanding of IoT is essential for utilising its benefits and developing effective security action to protect such a network. The growing integration of IoT devices into daily life and industrial processes has created unprecedented opportunities for innovation. However, with this growth comes the responsibility to ensure that such devices and the networks they form are secure from cyber threats.

5G networks represent the latest mobile communication technology. They are designed to improve wireless network speed, latency, and connectivity. Unlike old generations, 5G networks are not merely an upgrade but a revolutionary leap forward. They allowed new use cases such as increased mobile broadband, ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC). These capabilities support the burgeoning Internet of Things (IoT) eco-environment system. Devices in this eco-environment system require reliability, secure communication, and fast communication channels to operate effectively. 5G networks offer a range of benefits. They provide high data rates of up to 10 Gbps, latency as low as 1 millisecond, and the ability to connect a range of up to one million devices per square kilometre. All these features make the 5G a foundational technology for the upcoming generation of IoT applications. Real-time data processing, autonomous systems, and smart city infrastructure depend on ultra-fast and reliable network connections. The motivation for understanding and adopting 5G technology lies in its potential to address the limitations of old communication networks. It unlocks new possibilities for IoT. As the number of connected devices grows exponentially, a network that can handle vast amounts of data with minimum delay is essential. 5G is positioned to meet these demands. It allows fast internet speed and supports advanced IoT applications requiring real-time processing and decision-making. Next, 5 G is increasing the security features, such as stronger encryption and improved authentication mechanisms, which are vital for protecting IoT networks from emerging cyber threats. The importance of security in IoT devices cannot be overstated. These devices are integrated into complex infrastructure and industrial systems. They range from simple sensors to complex machinery and are often connected to networks via the Internet. This connectivity makes them susceptible to a wide array of cyber threats. These threats include unauthorised access, data breaches, and distributed denial-of-service (DDoS) attacks. Such attacks can disrupt device functionality. As IoT devices become more prevalent, the potential impact of security breaches escalates. Consequences can affect individual privacy, business operations, and national security [3]. One of the key challenges in securing IoT devices is their inherent diversion. IoT device has varied levels of processing of power, memory, and communication capabilities. These diversities make it challenging to implement standardized security measures across all devices. Many IoT devices prioritize functionality and cost-efficiency over robust security features. This focus on functionality has led to an increasing number of vulnerabilities. A malicious person can exploit these vulnerabilities [3].

In healthcare, IoT devices monitor the health of patients in real-time. A compromise in these devices could lead to a life-threatening situation. In industrial settings, IoT devices control and monitor complex processes. A security breach in these systems could result in operational disruption, physical damage, and financial losses. As reliance on IoT technology increases, ensuring the security of these devices is essential. Maintaining trust in digital systems and preventing catastrophic failures is critical [3]. Moreover, the interconnected nature of IoT ecosystems means that the compromise of a single device can have consecutive effects. This could jeopardize the entire network. Therefore, security measures must be proactive, scalable, and adaptable to the evolving threat landscape. Addressing the importance of security in IoT devices highlights the need for a comprehensive security framework. This framework should encompass device authentication, data encryption, secure communication protocol, and regular software updates [3]. The significant contribution of this work is as follows:

1. Provide a novel Knowledge of cyber threats specific to IoT devices.
2. Comparative analysis of ML, DL, FL, and EA techniques in IoT security.
3. Give real-world practical case studies for the effectiveness of CI techniques.
4. Identification of key research challenges and future directions in IoT security.

2. Fundamentals of Computational Intelligence Techniques

2.1 Evolution of Computational Intelligence Techniques: - Computational Intelligence (CI) techniques have evolved significantly over the last few decades. They have transformed from basic algorithms into complex models. These models now power many applications, especially in IoT hardware security. The evolution of CI techniques can be traced through several key stages. Advances in computational power mark each stage. Algorithmic innovation has also played a critical role. Additionally, the integration of interdisciplinary knowledge has driven this evolution [4].

a) **Early Stages: Rule-Based Systems and Expert Systems:** In the early stages, computational intelligence focused mainly on rule-based and expert systems. Knowledge was encoded into a set of rules that machines could follow. These systems

relied heavily on human expertise. They could only handle predefined scenarios. This limitation affected their adaptability and scalability.

b) **Introduction of Fuzzy Logic (1965):** Fuzzy logic, introduced by Lotfi Zadeh in 1965, was a breakthrough in CI. Unlike binary logic, which deals with true or false values, fuzzy logic allows for degrees of truth. This enables systems to handle uncertainty and approximate reasoning. It was instrumental in control systems and decision-making processes where binary decisions were insufficient.

c) **Emergence of Neural Networks (1980s):** The 1980s brought renewed interest in neural networks inspired by the structure of the human brain. These networks can learn from data through processes like backpropagation. Backpropagation enabled them to model complex, non-linear relationships. This era marked the start of CI techniques that could learn and adapt to new information without explicit programming.

d) **Advancement with Evolutionary Algorithms (1990s):** The 1990s introduced evolutionary algorithms inspired by natural selection principles. Techniques like genetic algorithms and genetic programming gained popularity. These were effective for optimization problems where traditional methods fell short. Evolutionary algorithms could evolve solutions over time. This made them powerful tools for search and optimization in dynamic environments.

e) **Rise of Machine Learning (2000s):** The early 2000s saw the rise of machine learning. This period introduced support vector machines, decision trees, and ensemble methods. Machine learning algorithms could automatically learn patterns from large datasets. This made them ideal for applications like image recognition, natural language processing, and predictive analytics.

f) **Deep Learning Revolution (2010s):** The 2010s experienced the deep learning revolution. This was driven by advancements in computational power and the availability of large datasets. Innovations in neural network architectures, such as CNNs and RNNs, play a key role. Deep learning models achieved unprecedented accuracy in speech recognition, object detection, and language translation tasks.

g) **Integration of Hybrid Systems (2020s and beyond):** The current era is marked by the integration of hybrid systems. These systems combine multiple CI techniques to leverage their strength. For instance, deep learning is often paired with fuzzy logic to handle uncertainty. It is also combined with an evolutionary algorithm for optimization. This hybrid approach is highly effective in critical IoT environments. Here, diverse and evolving threats require adaptive and intelligent security solutions.

2.2 Use Cases in IoT Security: The integration of Internet of Things (IoT) devices across several sectors has brought about many advantages. It has also introduced significant security challenges and issues. As devices are increasingly deployed in critical systems, securing them becomes the most important. Securing IoT devices is crucial to ensure data and operations' integrity, availability, and confidentiality. Several use cases with examples of the importance of IoT security [5].

a) Healthcare

- **IoT Use Case:** In healthcare, IoT devices such as smart medical equipment, wearable health monitor systems, and connected implants collect and transmit patient data in real-time. These devices enhance patient care by enabling remote monitoring and timely mediation.
- **Security Challenge:** The security of these devices is critical because unauthorized candidate access or data breaches can lead to serious consequences. Including the alteration of medical data, which is the result of incorrect treatment. Insecure devices may also be vulnerable to attacks that could lead to device malfunction. Posing the risks to safety of patient.
- **Solution:** Implementation of end-to-end encryption, high authentication protocol, and continuous monitoring of IoT devices are essential strategies to ensure data integrity and protect patient information.

b) Smart Cities

- **IoT Use Case:** Smart cities utilize IoT devices to manage the urban infrastructure. Including traffic lights, water supply, and public transportation. These devices contribute to the good management of resources and improve the quality of life for residents in smart cities.

- **Security Challenge:** The interconnecting of IoT devices in smart cities makes them susceptible to cyber-attacks. For instance, compromising the traffic management system could lead to road chaos, while the water supply system attack could disrupt most services.
- **Solution:** To secure the smart city infrastructure. It is a vital role to deploy multi-layered security systems. That includes network segmentation, anomaly detection systems, and secure communication channels to prevent unauthorized access and ensure the smooth functioning of city services.

c) Industrial IoT (IIoT)

- **IoT Use Case:** In industrial settings, IoT devices monitor and control machinery, track production processes, and optimize supply chains. IIoT enables predictive maintenance, reducing downtime and improving efficiency.
- **Security Challenge**: The industrial sector faces unique security issues because a breach in the IIoT system can lead to operational disruption, financial loss, and even physical damage. The integration of legacy systems with modern IoT devices also introduces drawbacks to the system.
- **Solution:** Industrial IoT security requires a combination of network security measures, such as firewalls and intrusion or virus detection systems. Furthermore, device-specific protection is needed, such as a secure boot mechanism and regular firmware updates. Additionally, adopting the zero-trust security mechanism helps minimise the risk of falling out.

d) Smart Homes

- **IoT Use Case:** Smart home devices, such as thermostats, lighting systems, security cameras, and smart locks, offer convenience and energy efficiency by allowing users to control and automate various aspects of their homes.
- **Security Challenge**: The widespread adoption of smart home devices introduces privacy risks and the potential for unauthorized access to personal data. For example, a breach in a smart lock system could allow unauthorized entry into a home, while compromised security cameras could lead to privacy invasions.
- **Solution**: Securing smart home devices involves implementing strong encryption, ensuring devices receive regular updates, and educating users about safe practices, such as using strong, unique passwords and avoiding unsecured networks.

e) Automotive IoT

- **IoT Use Case**: The automotive industry employs IoT in connected vehicles for features such as advanced driver-assistance systems (ADAS). In vehicle infotainment and vehicle-to-everything (V2X) communication system. These features increase the feeling of safety and driving experience.
- **Security Challenge**: Connected vehicles are vulnerable to cyber threats that could compromise their safety features. Leading to an accident on the runway or an unauthorized person to track the vehicle's location. The complexity of automotive IoT systems makes securing every component a challenging task.
- **Solution:** Ensuring automotive IoT security involves implementing a high encryption system. Secure communication protocol and continuous security testing throughout the vehicle's lifecycle. Collaboration between hardware manufacturers, software developers, and security experts is essential to develop collective security solutions.

2.3 Significance in Enhancing IoT Security:

Enhancing the security of the Internet of Things (IoT) is of utmost importance. The growth and wide use of IoT devices are significant. These devices are present in several sectors, such as healthcare systems, industrial systems, smart city projects, and consumer electronics. IoT devices often connect to the internet and each other. They handle vast amounts of data. They also control the complex infrastructure and interact with sensitive personal information. As a result, securing IoT devices is more than just a technical necessity. It is a foundational requirement. This ensures trust, privacy, and the reliability function of the digital environment [5].

a) Protection of Sensitive Data

IoT devices frequently collect, store, and transmit sensitive data. This data can include personal health information on wearable devices. It can also involve financial transactions of smart payment systems. Compromise of such data can have serious con-

sequences. It can lead to identity theft, economic loss, and security breaches. Therefore, increasing IoT security is crucial. It helps protect against unauthorized access, data breaches, and other cyber threats. Many strategies are essential for safeguarding sensitive information handled by IoT devices. Encrypting the data in transit and at rest is crucial. A higher authentication model is also necessary. Furthermore, the implementation of secure communication protocols is vital.

b) Ensuring Operational Continuity

In critical sectors such as healthcare and industrial systems, uninterrupted operation of IoT devices is vital. A security breach in this environment can have serious consequences. It can disrupt services, cause operational downtimes, or even lead to physical losses. For example, an attack on IoT devices controlling industrial machinery could stop the production lines. A breach in medical IoT devices could negatively impact patient care. Increasing IoT security is essential to maintain uninterrupted operation. Regularly updates the critical factor. Implement the intrusion detection systems is also necessary. Additionally, redundancy planning helps these devices resist attacks and continue functioning without disruption.

c) Mitigating Emerging Threats

As IoT devices increase in number, cyber-attacks are also becoming more experienced. Attackers are increasingly targeting IoT devices. They use them to launch a Distributed Denial of Service (DDoS) attack. They also exploit device vulnerabilities for unauthorized surveillance. In more cases, they hijack devices for malicious activities. Enhancing the security in IoT is critical. It helps to stay ahead of these evolving attacks. Protecting both individual devices and the broader network system is the most important. Adopting advanced security techniques is vital in IoT systems. Machine learning can be used for malicious activity detection. Artificial intelligence-driven attack hunting is also essential. Furthermore, automated sudden response plays a crucial role. These measures help identify and mitigate new and emerging attacks.

c) Maintaining User Trust

User trust is critical for the widespread adoption and success of IoT technologies. A security incident such as breaches or unauthorized persons accessing IoT devices can damage this trust. As a result, users may become reluctant to adopt new technologies. IoT devices are deeply integrated into daily life items in such sectors as smart homes or consumer electronics. In this area, maintaining security is directly linked to user confidence. Several measures are essential to support and increase user trust in IoT systems. Transparent security practices are essential. Educating users about security is also a vital key role.

d) Regulatory Compliance

Several regions are enacting strict regulations on data protection and device security. This is especially true for IoT devices that handle personal or crucial data. Compliance with these regulations is not just a legal requirement. It is also a major driver of improved security practices. Non-compliance can lead to serious consequences. These include legal penalties, financial loss, and damage to an organization's reputation. Organizations must implement security frameworks that align with relevant regulations. Examples include the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States. This involves adopting standardized security measures issues. Regular security audits are also necessary. Additionally, it is essential to ensure that all IoT devices meet regulatory requirements.

2.4 Standardization Efforts: As the Internet of Things (IoT) grows, billions of devices are connected to worldwide networks. The need for standardized security measures is becoming increasingly crucial. Standardization effort's main aim is to create uniform guidelines and protocols. These ensure IoT devices' security, interoperability, and scalability across various platforms and industries. Such efforts are essential for fostering innovation. They also enable global collaboration. Furthermore, they will help to mitigate the different security challenges posed by the fast growth of the IoT environment [6].

a) International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is leading in creating standards for IoT security. One of the key standards is ISO/IEC 27001. This standard provides the framework of information security management systems (ISMS) that can be used in IoT systems. Another necessary standard is ISO/IEC 30141. This standard establishes IoT reference architecture with consideration of security. It promotes a shared understanding and approach to IoT security across several sectors. These

standards can help organizations implement strong security measures. They ensure that IoT devices and systems are protected from several cyber-attacks, following ISO standards, and supporting global trade and cooperation. This is achieved by ensuring that products meet internationally recognized security criteria. Implementing ISO standards helps organizations maintain a high level of security. This reduces the risk of breaches. It also ensures compliance with regulatory requirements.

b) Institute of Electrical and Electronics Engineers (IEEE)

The IEEE has developed different standards focused on IoT security. One notable standard is IEEE 802.15.4. This standard supports low-rate wireless personal area networks (LR-WPANs). It includes the essential security features for IoT devices that can use wireless communication. Another necessary standard is IEEE P2413. This standard provides the architectural framework for IoT systems. It can address security and privacy concerns at several layers of IoT systems. IEEE standards are widely adopted in the industry. They ensure that IoT devices can communicate securely within several networks. These standards support the creation of secure and interoperable IoT solutions. Such solutions can be deployed across different industries. Additionally, IEEE standards increase the security of IoT devices. This ensures they are resistant to common cyber-attacks. It also guarantees secure communication.

c) European Telecommunications Standards Institute (ETSI)

The European Telecommunications Standards Institute (ETSI) is the critical standardizing IoT security. There is a focus on especially telecommunications. ETSI's Technical Committee on Cyber Security (TC CYBER) has been created to various essential standards. One of the key standards is ETSI TS 103 645. This standard provides a baseline for IoT security. It covers the areas such as device identity and data protection. ETSI standards are significant for the European market. Compliance with these guidelines is more required for market access in Europe. ETSI's emphasis on telecommunications ensures that IoT devices can be securely connected. This is essential within complex network systems. ETSI standards help ensure that IoT devices in Europe have crucial security features. This reduces the risk of vulnerabilities. It also ensures compliance with regional regulations.

d) Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) has developed key protocols for securing IoT devices. Notable among these is the Datagram Transport Layer Security (DTLS) protocol in IoT. DTLS provides communication security for IoT devices. Next, the critical protocol is the Constrained Application Protocol (CoAP). CoAP includes security features designed for resource constrained IoT environments. IETF's protocols are widely used in IoT systems. They are providing a foundation for secure communication over the Internet. These protocols are designed to work efficiently in IoT environments with limited resources. This makes them free for IoT applications. Adopting IETF protocols ensures that the IoT devices can be securely communicated over the networks. It can help protect data in transit. It also provides the integrity of communications between devices.

e) National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) in the United States have developed and provided various IoT security guidelines and frameworks. NIST's Cyber Security Framework (CSF) offers a comprehensive approach to managing cyber security risks in IoT systems. NIST has also published special publications such as NIST SP 800-183. This publication addresses network security for IoT systems. NIST standards are highly regarded both in the United States and globally. They serve as a benchmark for best practices in IoT security. Organizations following the NIST guidelines are better equipped to manage cyber security attacking risks. It can be better to protect their IoT deployments. Implementing the NIST standards helped organizations increase their IoT systems' security. It ensures that it can be identified, protected against, detected, responded to, and recovered from cyber security incidents [20].

3. Taxonomy of Cyber Threats Targeting IoT Devices

IoT devices continue to proliferate across different sectors. They become increasingly attractive targets for cyber security criminals. They have unique characteristics of IoT devices, such as their limited processing power and diverse range of applications. Also, insecure network configurations make them vulnerable to various cyber-attacks. A comprehensive taxonomy of

these threats is essential to understanding the security challenges inherent in IoT environments and developing efficient counter-measuring [21].

3.1. Overview of IoT Device Vulnerabilities

- **Insecure Communication Protocols:** Many IoT devices use insecure or outdated communication protocols. These protocols may lack encryption or authentication features. The device is susceptible to interception, man-in-the-middle (MitM) attacks, and data breaches. Commonly targeted protocols include HTTP, FTP, and Telnet. These protocols are still used in many IoT deployments despite their well-known challenges.
- **Lack of Regular Updates:** IoT devices are repetitive and run-on outdated firmware and software due to the lack of regular updates or the complexity of managing updates. This makes them vulnerable to known exploits and zero-day challenges (V14I3-5 (1)).
- **Weak Authentication Mechanisms:** IoT devices are shipped with default or not strong passwords that users do not change. Making them easy targets for brute-force attacks. Next, some devices cannot enforce strong password policies, exacerbating this vulnerability.
- **Insufficient Physical Security:** IoT devices deployed in public or unprotected areas may lack physical security analysis. Making them vulnerable to tampering, theft, or unauthorized access. Physical access to a device can allow an attacker to bypass software protection and directly exploit hardware challenges.

3.2 Classification of Cyber Threats [22]

Malware Attacks:

Botnets: IoT devices are more recruited into botnets. These botnets are used to conduct the Distributed Denial of Service (DDoS) attacks. A notable example is the Mirai botnet. The Mirai botnet compromised thousands of IoT devices. Botnets exploit weak authentication mechanisms and default credentials to take control of devices.

Ransomware: It is more common in traditional IT environments for ransomware attacks on IoT devices. This is particularly true in sectors like the healthcare system. Connected devices, such as smart medical equipment, can be locked down. Attackers are demanding ransom for the release of these devices.

Denial of Service (DoS) Attacks: Prime targets of IoT devices for DDoS attacks due to their limitation of resources. Attackers flood the device or network traffic. This causes the device or network to be unavailable to legitimate users. DDoS attacks can be catastrophic in crucial infrastructure systems, such as smart grids or industrial controlling systems.

Physical Attacks: Physical tampering in IoT devices can give the attackers unauthorized access. It can also allow them to implant viruses directly with the device. For example, tampering with a smart meter and gadgets could alter the reported energy consumption. This can lead to financial losses or disruptions in energy distribution.

Side-Channel Attacks: These attacks exploit the physical implementation of a device rather than the software. It may involve power of consumption measuring or electromagnetic emissions. The goal is to extract sensitive information, such as the cryptographic keys.

Data Breaches and Privacy Violations: IoT devices repetitively transmit sensitive data over unencrypted channels. This makes it easy for attackers to intercept communication and access private information. This is particularly concerning with the IoT healthcare devices that transmit patient data.

Data Exfiltration: A compromised IoT device can exfiltrate sensitive data to a network. For example, smart home devices such as security cameras can be exploited. They may leak the private footage or user credentials to external attackers' persons.

3.3 Key Security Concerns in IoT Environments

Scalability of Security Solutions: The Number of IoT devices is growing exponentially. Ensuring that the scale of security solutions can be efficient is a significant concern. Many old security measures are not readily applicable to the vast and diverse IoT devices due to their constrained resources and heterogeneous nature.

Lack of Standardization: The absence of universal security standards for IoT devices leads to inconsistent security practices across the manufacturer's systems, industries, or companies. This fragmentation makes implementing the comprehensive security strategies challenging and leaves many device issues to standard attack (V14I3-5 (1)).

Interoperability Issues: IoT systems involve devices from multiple vendors with diverse security capabilities. Ensuring the devices can be securely communicated and operate together without introducing challenges is a significant challenge.

Privacy Risks: IoT devices often collect and transmit large amounts of personal data. Increased significant privacy concerns. Ensuring that this data is adequately protected from unauthorized accessing or misuse is crucial to maintaining user trust and compliance with data protection regulations.

4. Application of Computational Intelligence Techniques in IoT Security

The fast growth of the Internet of Things (IoT) has introduced critical security issues that traditional cybersecurity methods often struggle to address. Computational Intelligence (CI) technique, Machine Learning (ML), Deep Learning (DL), Fuzzy Systems, and Evolutionary Algorithms have emerging techniques as powerful tools for increasing IoT security. This technique can process vast amounts of data, change the environment, and provide intelligent responses to different security attacks.

4.1 Machine Learning for IoT Security

Overview of ML Techniques: Machine Learning includes algorithms that allow systems to learn patterns from data and make decisions with negligible human intervention. In IoT security, ML models such as supervised, unsupervised, and reinforcement learning are commonly used to detect anomalies, classify threats, and predict potential security breaches.

Applications in Threat Detection: Machine Learning has proven effective in detecting several types of cyber-attacks in IoT environment systems. For instance, anomaly detection algorithms can identify unusual patterns in network traffic, which may indicate the presence of malicious activity. One common approach is using Support Vector Machines (SVM) for binary classification of normal and abnormal behavior in IoT hardware devices.

Mathematically, if we define a dataset $X = \{x_{1,}x_{2,}x_{3,} \dots \dots . x_{n,}\}$ where each x_iIs a vector feature, and the corresponding labels are$y = \{y_{1,}y_{2,}y_{3,} \dots \dots . y_{n,}\}$, SVM's objective is to find the hyperplane that maximizes the margin between the two classes. The decision function f(x) is given that:

$$f(x) = \text{sign}\left(\sum_{i=1}^{n} a_i\, y_i\;\; K(x_i, x) + b\right)$$

Where a_i the Lagrange of the multiplier is, $K(x_i, x)$ is the kernel function, and b is the bias term. This decision function helped classify the input vector feature as either standard or anomalous, aiding in the detection of potential security attacks.

4.2 **Deep Learning for IoT Security**

Overview of DL Techniques: Deep Learning is a subset of Machine Learning that uses a neural network with multiple layers to design a model of complex data set pattern. Neural network techniques such as Convolution Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are instrumental in examining sequential and high-dimensional data commonly used in IoT environments.

Case Studies in Anomaly Detection: Deep Learning has been successfully applied to anomaly or virus detection in IoT security. For example, a neural network can be trained to reconstruct regular data patterns. When anomalies occur, the reconstruction error is typically high, signaling the presence of malicious activity. The reconstruction of error $e(x)$Can be mathematically presented as:

$$e(x) = \| x - x\hat{} \|^2$$

Where x is the input data and $x\hat{}$ is the reconstructed output from the Autoencoder. A high value of $e(x)$ indicate an anomaly or viruses.

4.3 **Fuzzy Systems in IoT Security**

Introduction to Fuzzy Logic: Fuzzy Logic extends classical logic by allowing reasoning with degrees of truth rather than binary true/false or 1/0 values. This is particularly useful in IoT security, where decisions often must be made in uncertain circumstances. A Fuzzy Inference System (FIS) uses fuzzy sets and rules to derive conclusions from summarized data.

Use Cases in Decision Making: Fuzzy Systems can be used to analyze the device's risk level based on several factors such as device behavior, network condition, and historical data. For example, if $\mu low(x), \mu medium(x), and\ \mu high(x)$ represent the memberships function for low, medium, and high-risk levels. The overall risk $R(x)$ can be calculated as:

$$\mathrm{R(x)} = \frac{\mu\mathrm{low(x)} \times 1 + \mu\mathrm{medium(x)} \times 2 + \mu\mathrm{high(x)} \times 3}{\mu\mathrm{low(x)} + \mu\mathrm{medium(x)} + \mu\mathrm{high(x)}}$$

This risk assessment can guide security decisions, such as quarantining a device or initiating further investigation.

4.4 **Evolutionary Algorithms for IoT Security**

Evolutionary Algorithms: Evolutionary Algorithms (EAs) are optimization techniques motivated by natural selection. These algorithms iteratively expand the population of candidate solutions toward an efficient solution. Genetic Algorithms (GAs) and Particle Swarm Optimization (PSO) are common EAs used in IoT security for detection systems and designing a better security protocol.

Applications in Intrusion Detection: Evolutionary Algorithms can be used to optimize the parameters of intrusion detection systems (IDS). For instance, a Genetic Algorithm might expand the rules IDS uses to maximize the accuracy and minimize false positives rate. The fitness function $f(P)$ for a population P of candidate solution expressed as:

$$f(P) = \sum_{i=1}^{n} (\mathrm{Accuracy(Pi)} - \lambda \times \mathrm{False\ Positives(Pi)})$$

Where λ is a weighting factor that balances the trade-off between accuracy and false positives rate. The best-performing solutions are selected for reproduction in the upcoming generation. Leading to increasingly effective IDS configuration systems.

5. Case Studies and Practical Examples

5.1 Successful Applications of Computational Intelligence in IoT Security

Computational Intelligence (CI) techniques have been successfully applied in several IoT security scenarios. Demonstrating their effectiveness in mitigating cyber-attacks. These applications range from virus detection systems to advanced intrusion detection frameworks, employing several Machine Learning (ML), Deep Learning (DL), Fuzzy Logic, and Evolutionary Algorithm to be applied. For example, the case study involves smart home devices. ML algorithms were implemented to detect Distributed Denial of Service (DDoS) attacks. The study utilized a Support Vector Machine (SVM) supervised machine learning technique to classify network traffic data into standard and attack categories. The decision boundary of the SVM can be mathematically represented as the following equation:

$$f(x) = \sum_{i=1}^{n} a_i\, y_i\, K(x_i, x) + b$$

Where a_i are the Lagrange multiplier, y_i are the class label, $K(x_i, x)$ is the kernel function, and b is the bias term. The effectiveness of the SVM model was validated using various metrics such as accuracy, precision, recall, and F1-score, providing its capability to detect and prevent DDoS attacks in real time.

5.2 **Analysis of Real-World Scenarios**

IoT allows a smart grid to be analyzed to assess the application of the deep learning technique for anomaly detection. Convolution Neural Networks (CNNs) were employed to monitor data streams from sensors within the grid. The CNNs input data

processing, collecting the feature maps, and detecting anomalous patterns. The output of the final layer was used to classify the input as either standard or an anomaly. The activation function used in the final classification layer can be presented as:

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

Where z is the weighted sum of input. This sigmoid activation function outputs a probability value range between 0 to 1. Indicate the input data as being anomalous. The study demonstrated that CNNs could significantly reduce the false positives rate while maintaining high detection rates, thus improving the smart grid's overall security.

Next, Fuzzy Logic was applied in IoT security to handle the uncertainty in sensor data from smart city data. In one case study, a Fuzzy Inference System (FIS) was developed to analyze the risk levels of IoT devices based on multi-criteria such as device behavior, network traffic, and historical data. The fuzzy rules were presented as follows:

$$\text{IF x1 is High AND x2 is Low THEN Risk is Medium}$$

Where x_1 and x_2 represent input variables such as traffic volume and device reputation. The output risk level was calculated using fuzzy membership functions and defuzzification techniques, providing a flexible approach to managing IoT security.

In another example, the Evolutionary Algorithm was applied to optimizing industrial IoT network intrusion detection systems (IDS). The Genetic Algorithm (GA) evolved the detection rule over various generations, improving the system's accuracy and minimizing false favorable rates. The fitness function for the GA can be expressed as follow:

$$f(P) = \sum_{i=1}^{N} (\text{Accuracy}(Pi) - \lambda \times \text{False Positives}(Pi))$$

Where P represents the candidate population of solutions, λ is a weighting factor, and N is the population size. This optimization process led to the development of a more robust IDS capable of effectively protecting the industrial IoT network from several cyber-attacks.

6. New Challenges and Future Research Directions

6.1 Emerging Threats in IoT Security

The fast-growing landscape of the Internet of Things (IoT) introduces several new security issues exacerbated by the increasing complexity of cyber-attack. Emerging threats include advanced persistent threats (APTs), zero-day vulnerabilities, and large-scale botnet attacks, which leverage the vast number of connected IoT devices. These threats must be addressed through the development of more robust security measures. One of the critical issues is the detection and mitigation of zero-day attacks. The probability $P(compromise)$ that a zero-day vulnerability in an IoT device will be exploited can be modeled as follows:

$$P(\text{compromise}) = 1 - \prod_{i=1}^{N} (1 - p_i)$$

Where p_i represents the probability of exploitation for every vulnerability i, and N is the total number of vulnerabilities. This equation highlights the risk posed by multiple vulnerabilities in IoT devices, emphasizing the need for continuous monitoring and fast response mechanisms.

6.2 Limitations of Current Computational Intelligence Techniques

Despite the advancements in Computational Intelligence (CI) for IoT security, various limitations still hinder their effectiveness. For instance, classical Machine Learning (ML) models require substantial labeled data to maintain high accuracy, which is often unavailable or impractical to obtain in IoT environments. The following learning curve provides a mathematical representation of these models' performance:

$$\text{Error}(\text{m}) = \frac{\sigma^2}{\text{m}} + \epsilon$$

where σ^2 denotes the variance of the estimator, m is the several training examples, and ϵ is the irreducible error. This equation demonstrates the inverse relationship between the several training examples and the model's error rate, indicating the need to be present for large datasets to enhance model performance. Furthermore, while strong, deep learning (DL) techniques frequently require computational intensiveness and significant resources, which are limited in numerous IoT devices. The training time T of a deep learning model is proportional to:

$$\text{T} \propto \text{n} \times \text{d} \times \text{e}$$

Where n is the number of neurons, d is the number of layers, and e is the number of epochs. This relationship indicates that a more complex model with deeper architectures can be prohibitive for real-time IoT applications due to their computational requirement.

6.3 **Future Trends in Enhancing IoT Security**

Future development in IoT security is likely to incorporate the hybrid of more advanced CI techniques and hybrid models that combine the strength of multiple approaches. Federated Learning (FL) is emerging as a promising IoT security technique, enabling distributed devices to learn a shared model while keeping data localized collaboratively. The global model w_tAt iteration t in federated learning is updated as:

$$w_{t+1} = \eta \sum_{\text{k}=1}^{\text{K}} \frac{\text{n}_\text{k}}{\text{N}} \nabla \text{F}_\text{k} \, (w_t)$$

Where η is the learning rate, K is the number of devices, n_k is the number of data points at device k, N is the total number of data points, and ∇F_k represent the gradient computed at device k. These approaches improve privacy and reduce the risk of data breaches, making them highly relevant for IoT environment systems. Additionally, Quantum Machine Learning (QML) is expected to revolutionize IoT security by leveraging the principles of quantum computing to solve complex problems more efficiently. The ability of QML in processing huge amounts of datasets and identifying patterns in IoT-generated data could significantly enhance the detection and response to cyber-attacks. The evolution of these techniques will require increased research to overcome current limitations. Address the unique challenge posed by IoT environments.

Table 1: Comparative Analysis of CI Techniques

Technique	**Strengths**	**Limitations**	**Suitability for IoT Security**
Machine Learning (ML)	Adaptable to various threats, real-time detection	Requires large datasets for training	Suitable for anomaly detection and predictive security
Deep Learning (DL)	High accuracy, automated feature extraction	Computationally expensive	Effective for intrusion detection and malware analysis
Fuzzy Logic (FL)	Handles uncertainty, interpretable decisions	Requires expert-defined rules	Useful for risk assessment and decision-making systems
Evolutionary Algorithms (EA)	Optimizes security policies, adaptive solutions	High computational cost	Suitable for optimizing security protocols and attack response mechanisms

7. Conclusion

The security of Internet of Things (IoT) devices is an ever-growing concern in our increasingly connected to the real world. This paper has highlighted the critical importance of securing these devices in the landscape of rising cyber threats. We have

explored the drawbacks inherent in IoT environments and the substantial role of Computational Intelligence (CI) techniques in enhancing IoT security. Through a detailed examination, we have learned how to use Machine Learning (ML), Deep Learning (DL), Fuzzy Logic, and Evolutionary Algorithms to detect and mitigate security attacks effectively. Case studies and real-world examples provided compelling evidence of these techniques' success in protecting IoT systems. It also addressed emerging threats, such as advanced persistent threats, zero-day drawbacks, and current CI techniques' limitations. Despite these challenges, the potential for CI to evolve and solve these issues remains strong. Future trends, including Federated Learning and Quantum Machine Learning (QML), ensure revolution IoT security. Federated Learning's decentralized approach can increase data privacy and reduce breach risk, while QML could significantly boost threat detection speed and accuracy.

As the expansion of the IoT landscape continues, so will the complexity of security issues. The future of IoT security hinges on the continuous advancement of CI techniques. Embracing innovations like Federated Learning and Quantum Computing will be pivotal in increasing IoT system security. Future research should focus on developing lightweight CI models that operate efficiently on resource constrained IoT devices while ensuring accuracy and reliability. In conclusion, while IoT security poses a significant challenge, CI's evolving landscape offers a promising pathway to a more resilient and secure IoT ecosystem. We can better protect our interconnected world from emerging cyber-attacks by leveraging this advancement.

To address current limitations, future research should focus on:

- **Federated Learning for IoT Security**: Leveraging distributed ML models while preserving user privacy.
- **Quantum Machine Learning (QML):** Enhancing the computational efficiency of CI techniques for IoT.
- **Lightweight Security Solutions**: Developing CI models optimized for resource constrained IoT devices.
- **Adaptive Security Mechanisms:** Implementing self-learning algorithms that evolve with emerging threats.

Funding: "This research received no external funding"

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

References

[1]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, **Vol. 29, No. 7, pp. 1645–1660, 2013**.

[2]. J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5G be?" *IEEE Journal on Selected Areas in Communications*, **Vol. 32, No. 6, pp. 1065–1082, 2014**.

[3]. L. A. Zadeh, "Fuzzy sets," *Information and Control*, **Vol. 8, No. 3, pp. 338–353, 1965**.

[4]. S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: a survey," *Information Systems Frontiers*, **Vol. 17, pp. 243–259, 2015**.

[5]. R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, **Vol. 44, No. 9, pp. 51–58, 2011**.

[6]. ISO/IEC 30141:2018, *Internet of Things (IoT) – Reference Architecture*, International Organization for Standardization, **2018**.

[7]. C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, **Vol. 50, No. 7, pp. 80–84, 2017**.

[8]. A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, **Vol. 5, No. 4, pp. 586–602, 2017**.

[9]. M. S. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," *Proceedings of the IEEE World Congress on Services*, **2015, pp. 21–28**.

[10]. J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, **Vol. 17, No. 3, pp. 1294–1312, 2015**.

[11]. D. A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, and P. R. Inácio, "Security issues in cloud environments: a survey," *International Journal of Information Security*, **Vol. 13, No. 2, pp. 113–170, 2014**.

[12]. R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer Internet of Things devices,” *2018 IEEE Security and Privacy Workshops (SPW)*, **2018, pp. 29–35**.

[13]. L. Deng and D. Yu, *Deep learning: Methods and applications*, *Foundations and Trends in Signal Processing*, **Vol. 7, No. 3–4, pp. 197–387, 2014**.

[14]. L. A. Zadeh, “Fuzzy sets,” *Information and Control*, **Vol. 8, No. 3, pp. 338–353, 1965**.

[15]. D. E. Goldberg and J. H. Holland, “Genetic algorithms and machine learning,” *Machine Learning*, **Vol. 3, No. 2, pp. 95–99, 1988**.

[16]. N. Apthorpe, D. Reisman, and N. Feamster, “Closing the blinds: Four strategies for protecting smart home privacy from network observers,” *arXiv preprint arXiv:1705.06809*, **2017**.

[17]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, **Vol. 29, No. 7, pp. 1645–1660, 2013**.

[18]. D. M. Farid and C. M. M. Rahman, “Anomaly network intrusion detection based on improved self-adaptive Bayesian algorithm,” *Journal of Computers*, **Vol. 5, No. 1, pp. 23–31, 2010**.

[19]. J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, **Vol. 549, No. 7671, pp. 195–202, 2017**.

[20]. G. Shrivastava, S.L. Peng, H. Bansal, K. Sharma, M. Sharma, eds. New age analytics: Transforming the internet through machine learning, IoT, and trust modeling. CRC Press, **2020**.

[21]. M. Khari, G. Shrivastava, S. Gupta, R. Gupta. "Role of cyber security in today's scenario." In Detecting and mitigating robotic cyber security risks, IGI Global, pp. **177-191**, **2017**.

[22]. H. Sharma, P. Kumar, K. Sharma. "Recurrent Neural Network based Incremental model for Intrusion Detection System in IoT." Scalable Computing: Practice and Experience, **Vol. 25, no. 5, pp. 3778-3795, 2024**.