INVENTIVE DISCLOSURE - CONFIDENTIAL

1. Proposed Title of the Invention

Secure IoT Initialization and Encryption Framework Using Acoustic Signals and Criticality-Based Optimization

2. Proposed Abstract of the Invention

Current IoT systems tend to focus heavily on securing data as it leaves the peer-to-peer (P2P) network but often fall short when it comes to ensuring robust encryption within the network itself. Furthermore, they lack effective initialization protocols and apply uniform encryption standards, overlooking the varying importance of data and device criticality. This proposal outlines an innovative approach that uses a sound wave-based initialization process, paired with laser-assisted distance measurement, to fine-tune sound wave properties for secure and localized communication. The system introduces adaptive encryption that adjusts protection levels based on the sensitivity of the data and the importance of the device, while also implementing end-to-end encryption between individual IoT nodes and the central hub. To further bolster security, a partial zero-trust policy is employed, discarding any packets that originate from unverified sources or fail to meet expected formats. Designed with practical applications in homes, data centers, and healthcare environments, this framework not only addresses critical security challenges but also reduces computational demands, paving the way for more efficient and scalable IoT ecosystems.

3. Key Words:

Sound waves, Laser distance detection, IoT initialization, encryption, soundwave analysis, IoT device hierarchy, zero trust, Device Criticality, Risk Profiling, Data Sensitivity, Device Failure Risk

4. Background of the Invention:

What are the present technologies that exist in the field of your invention and what are the limitations of the same? (Present state of Art)

Table 1: Comparative Study

Name	**Description**	**Advantage**	**Disadvantage**
Light Weight Authentication Scheme for Smart Home IoT Devices [1]	This paper proposes a novel authentication mechanism that is specifically tailored for smart home IoT devices with limited computational and power resources. The approach emphasizes reducing overhead while maintaining robust security measures.	Energy-efficient design suitable for low-power devices; low computational overhead	Does not address device initialization using alternative channel such as acoustic methods; focuses solely on authentication rather than end-to-end secure onboarding.
Future Industry Internet of Technology with Zero-Trust security [2]	This paper presents a comprehensive framework for implementing zero-trust security in industrial IoT environments. It details how dynamic encryption and continuous validation can be integrated into existing infrastructures to enhance security.	Provides a robust and adaptable security model; support dynamic encryption based on device criticality; enhances protection in industrial settings.	Relies primarily on conventional wireless protocols for communications; does not incorporate innovative acoustic based initialization techniques.
A Novel Simplified AES Algorithm for Lightweight Real-Time Application: Testing and Discussion [3]	This work introduces a simplified version of the AES encryption algorithm optimized for real-time applications in resource-constrained environments. This paper includes performance testing and comparative discussion with standard AES implementations.	Offers improved efficiency and reduced latency; well-suited for devices with limited processing power; enhances real0time	Limited scope regarding secure device onboarding and initialization; does not integrate alternative communication

		encryption capabilities.	channels like acoustic signaling.
Revisiting Zero-Trust Security for Internet of Things [4]	This article revisits the principle of zero-trust security in the context of IoT systems. It discusses the challenges and potentials solutions for implementing continuous verification and trust evaluation across heterogenous IoT networks.	Provides in-depth theoretical and practical insights; highlights continuous authentication and verification; adaptable across various IoT environments.	Lacks focus on secure device pairing or onboarding process; does not explore acoustic-based initialization methods; primarily conceptual rather than implementation-focused.
Theory and Application of Zero Trust Security: A Brief Survey [5]	This survey provides an overview of zero-trust security model, discussing both theoretical foundation and practical application and practical application. It evaluates how zero-trust can be adopted to modern network environments, including IoT.	Offers a clear and broad theoretical background; identifies key benefits of zero-trust models; applicable to multiple domains including IoT.	Provides limited practical example specific to IoT device onboarding; does not integrate innovative secure initialization techniques such as acoustic signaling.
Power IoT Security Protection Architecture Based on Zero Trust [6]	The paper outlines a power-efficient security architecture for IoT that is based on zero-trust principles. It emphasizes balancing energy consumption with robust security, making it ideal for power-sensitive applications.	Scalable and robust design; optimizes energy consumption while ensuring high security; well-suited for power-sensitive and large-scale IoT deployments.	Scalable and robust design; optimizes energy consumption while ensuring high security; well-suited for power-sensitive and large-scale IoT deployments.

Zero Trust Real-Time Lightweight Access Control Protocol for Mobile Cloud-Based IoT Sensors [7]	This paper introduces a real-time access control protocol for mobile IoT sensors based on zero-trust principles. The protocol is designed to be lightweight and efficient, ensuring fast and secure communications in cloud-connected IoT systems.	Real-time responsiveness; low resource overhead; effective for mobile and cloud-based IoT sensor environments; ensures continuous authentication.	Does not incorporate novel methods for secure device onboarding such as acoustic initialization; limited to access control without addressing full device initialization processes.
ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Implementation [8]	This paper presents a novel architecture for IoT systems that leverages zero-trust security models. It includes a practical implementation and detailed performance evaluations, emphasizing secure communication and device management.	Provides a practical, implemented solution; enhances overall network security through zero-trust; supports dynamic encryption and continuous verification.	Does not address the use of alternative channels, such as acoustic signals, for secure device initialization; focuses on secure communication after device onboarding.
Acoustic Internet of Things Information Transmission System, Relay Base Station, and Method[9]	The patent describes an innovative system that employs acoustic signals for data transmission and device communication within IoT networks. It includes methods for signal generation, modulation, and reception.	Pioneers the use of acoustic channels in IoT communication; reduces reliance on electromagnetic methods; innovative approach to signal propagation.	Limited practical implementation details; performance can be affected by environmental noise; security aspects of initialization are not extensively addressed.

Ubiquitous Acoustic Sensing on Commodity IoT Devices: A Survey[10]	This survey reviews various acoustic sensing techniques employed in commodity IoT devices. It covers methodologies for data acquisition, processing, and application in different IoT scenarios.	Provides a comprehensive review of acoustic sensing methods; identifies potential applications in IoT; highlights the versatility of acoustic techniques.	Not specifically focused on secure initialization; lacks integration of dynamic encryption or zero-trust security models; more oriented towards sensing and data collection.

5. **What problems does the invention address and how your Invention is able to overcome the limitations/ problems of the existing technologies?**

   our IoT encryption and sound-based initialization framework addresses several limitations in pre-existing solutions, including-

   1. **Dependance on Conventional wireless protocols:** Traditional IoT systems heavily rely on wireless mediums like Wi-Fi and Bluetooth for initialization. They are highly susceptible to interference, spoofing and eavesdropping. Our framework eliminates this dependency by using inaudible acoustic signals, providing a secure and interference-resistant alternative.

   2. **Static Encryption Mechanisms:** Many current systems use one-size-fits all approach to encryption, lacking the ability to adapt based on the criticality of the device or data. Our hierarchy-based encryption adjusts the security levels based on the significance of the device and the data transmitted, ensuring optimal protection for high-priority nodes.

   3. **Lack of Precise Pairing Mechanisms:** Conventional methods often struggle with precise device pairing in environments with multiple devices. Our use of distance-calculated and superimposed directional acoustic waves ensures an accurate and targeted initialization, thus reducing pairing errors and cross-device interference.

   4. **Vulnerabilities to Insider and Unknown Threats:** Existing systems fail to adequately address internal threats or evolving attack vectors. By integrating a zero-trust policy, our framework ensures that all the interactions are verified, thus mitigating risks from both internal and external sources.

      By addressing these limitations, our system ensures robust security through inaudible acoustic signals and dynamic, hierarchy-based encryption tailored to critical nodes. It enhances efficiency with precise sound-based pairing and optimized energy usage, minimizing errors and resource consumption. This

versatile solution adapts seamlessly to diverse IoT devices, including resource-constrained environments.

6. Detailed Explanation of the Invention along with working examples. Kindly provide an elaborated description of each and every aspect of the invention (product and/or process) in great detail.

A. Invention Overview

Our invention presents a novel IoT onboarding and communication framework that utilizes acoustic signals for device initialization, combined with dynamic, hierarchy-based encryption and a zero-trust security model. This integrated solution is designed to enhance the security and efficiency of IoT networks by securely pairing devices and adapting encryption levels based on device roles and data sensitivity.

B. Acoustic-Based Initialization Process

At the core of the system is the use of acoustic signals—whose parameters are determined depending on the distance between the new node and the central hub—to transmit initialization data. When a new IoT device is introduced, it emits or receives these acoustic signals, which are precisely modulated based on the device's location and ambient conditions. The acoustic signal carries encrypted initialization parameters, including authentication keys, ensuring that only the targeted device can successfully decode and connect to the hub. Upon verification of the validity of the new node, credentials for joining the network are transmitted in the same manner.

C. Dynamic Hierarchy-Based Encryption

Following the initialization phase, the system employs an adaptive encryption strategy that assigns varying levels of cryptographic protection depending on each device's criticality (figure2). Devices that handle sensitive information or play a pivotal role in network operations are secured with advanced encryption algorithms, while less critical nodes are assigned standard encryption. This dynamic approach ensures that the overall network security is tailored to protect its most vulnerable points without compromising performance.

D. Zero-Trust Security Framework

Complementing the acoustic initialization and adaptive encryption is the implementation of a zero-trust security model. In this framework, no device is inherently trusted; every device and communication channel undergo continuous authentication and validation. This model protects the network from both external intrusions and potential internal breaches, ensuring that only verified entities are granted access to sensitive resources.

E. Communication and Control Mechanism

A centralized control unit orchestrates the entire initialization and encryption process. This unit is responsible for modulating the acoustic signals, processing device responses, and dynamically adjusting encryption parameters based on real-time network assessments. It acts as the nerve centre that manages secure communication between devices, ensuring that initialization and subsequent data transfers occur seamlessly and securely.

F. Hardware and Material Considerations

Key hardware components include precision ultrasonic transducers for generating and detecting inaudible acoustic signals, and robust microcontrollers integrated with encryption modules. These components are selected for their reliability and energy efficiency. Additionally, the design accommodates a compact form factor, ensuring that the system can be seamlessly integrated into diverse IoT setups without extensive modifications.

G. Working Example

Imagine a smart building where a new environmental sensor needs to join the network. Upon activation, the sensor emits an ultrasonic signal that is detected by the central control unit. Based on the sensor's spatial configuration, the control unit calculates optimal acoustic parameters and securely transmits initialization data. The sensor is then assigned a specific encryption level corresponding to its role, and continuous authentication under the zero-trust model ensures its communications remain secure.

H. System Monitoring and Flexibility

The central control unit continuously monitors the network for any deviations from expected behaviour. Real-time analytics allow the system to adjust encryption levels and acoustic parameters on the fly, providing flexibility to adapt to changes in network topology or emerging threats. This monitoring capability ensures that the system maintains a high level of security while adapting to evolving operational conditions.

I. Applications of the Invention

- **Smart Homes and Offices:** Secure and efficient onboarding of various IoT devices, such as sensors and smart appliances, while ensuring that critical devices receive enhanced protection.
- **Industrial IoT Networks:** Protection of sensitive industrial equipment and control systems by dynamically adjusting encryption levels and implementing continuous device authentication.
- **Healthcare Facilities:** Secure initialization and communication among medical devices, ensuring that patient data is protected against unauthorized access.

J. User-Friendly Adaptability

Designed with the end-user in mind, the system offers an intuitive interface that allows network administrators to easily configure initialization parameters, encryption hierarchies, and monitoring settings. This flexibility ensures that the framework can be customized to meet the specific security needs of different environments, making it a versatile solution for a wide range of IoT applications.

This detailed explanation illustrates how our invention seamlessly integrates advanced acoustic communication, adaptive encryption, and a robust zero-trust model to create a secure, efficient, and scalable IoT network solution.

7. Kindly attach drawings, reports, papers, charts or other materials that may aid in your description.

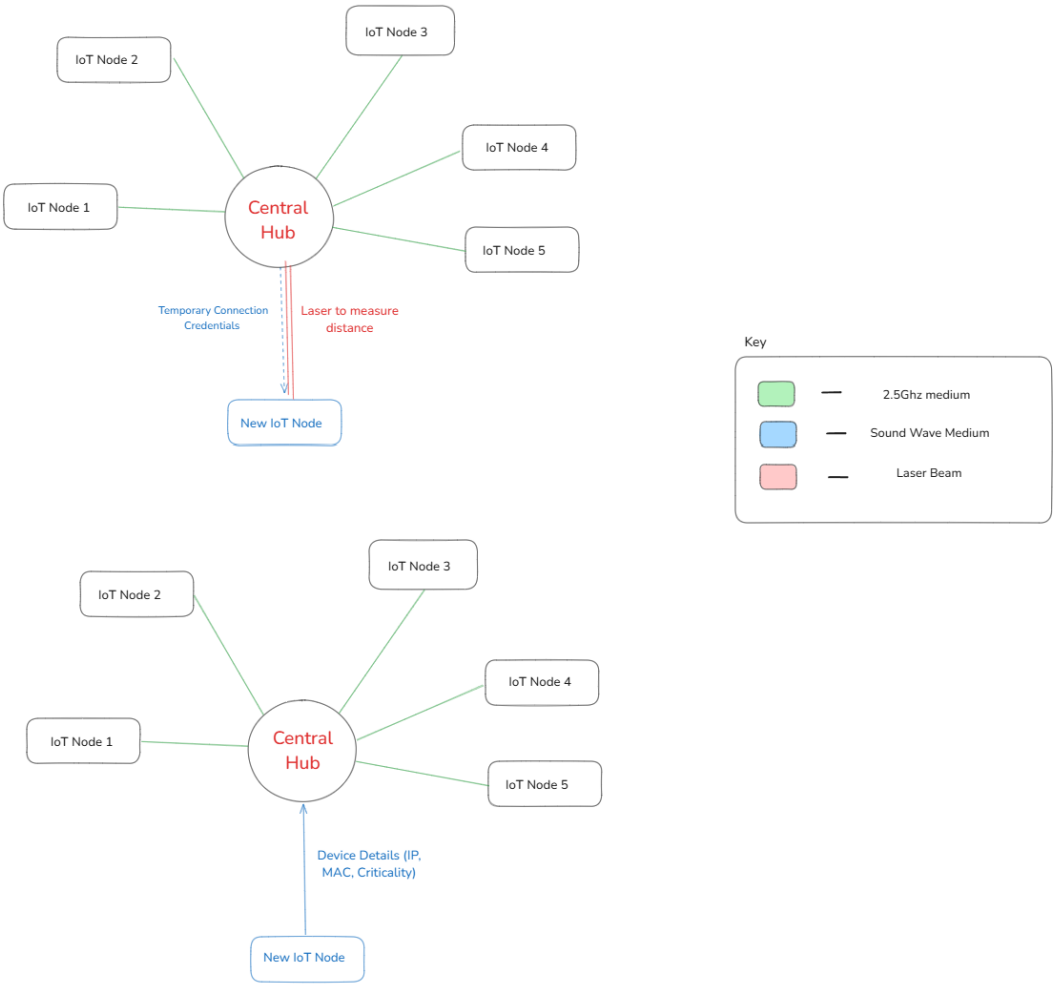

Figure 1a: Process Flow Diagram for the Initialization Sequence

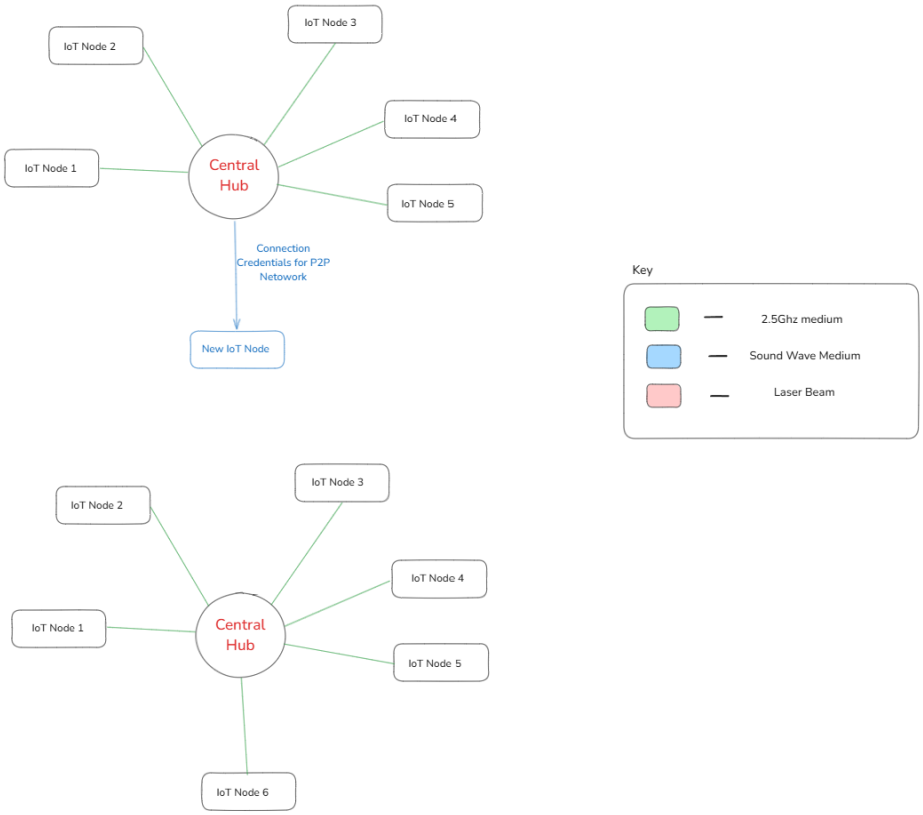

Figure 1b: Process Flow Diagram for the Initialization Sequence

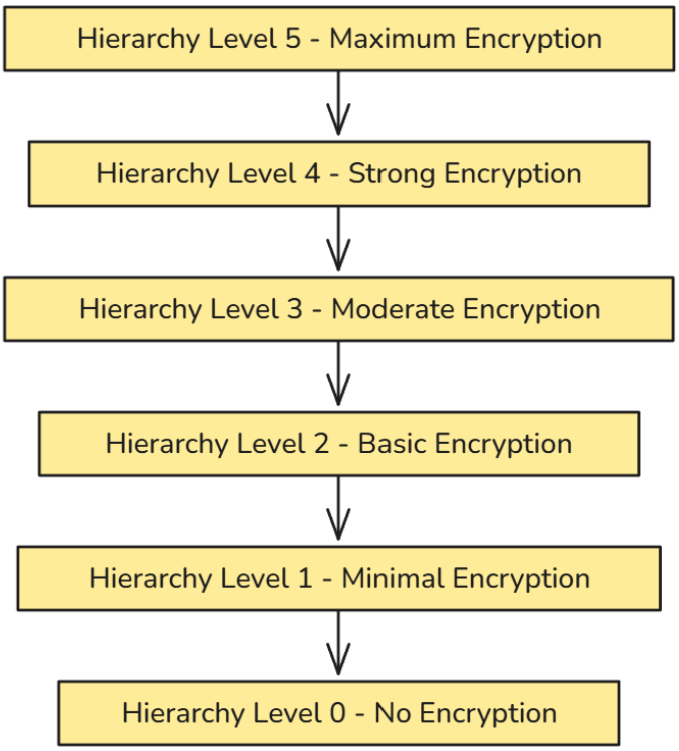

Figure 2: Different Levels of Encryption Hierarchy

8. What are the aspects of your disclosure that you want to claim/monopolize?

For our IoT encryption and sound-based initialization technique, we seek to claim and monopolize the following aspects:

1. **Sound-Based Initialization Process**: The use of inaudible acoustic signals for secure IoT device initialization, providing a reliable pairing method without reliance on conventional wireless protocols like Bluetooth or Wi-Fi. The acoustic wave parameters are dynamically calculated based on distance and precisely directed to the target device.

2. **Hierarchy-Based Encryption**: A dynamic encryption scheme that adjusts based on the criticality of nodes and data within the network, as well as their geographical location. Devices and data deemed high-priority are encrypted at a higher level, ensuring tailored security based on significance.
3. **Zero Trust Policy Integration**: The incorporation of a zero-trust policy in the framework, ensuring that no device or communication is implicitly trusted within the network. This approach mitigates threats by continuously validating all devices and data, regardless of their origin or internal position within the network.

9. Have you conducted a novelty/inventiveness search for your invention? If yes, what are the databases /references used by you? What are the search results?

Yes, an extensive search for novelty and inventiveness was carried out for our IoT encryption and sound-based initialization technique. We explored various databases, including Google Scholar, scientific journals, IPASS, Google Patents, IEEE Xplore, Elsevier, Springer, among others. This research covered both academic literature and patent databases to ensure a well-rounded evaluation of existing work in the relevant areas. The results highlighted a significant gap in current technologies. While there are some methods for audio encryption in IoT, such as the use of chaotic systems for encrypting audio signals under the MQTT protocol and secure short-range communication based on sound, none of these solutions closely resemble our proposed approach. Our technique uniquely combines IoT encryption with a sound-based initialization process, utilizing inaudible sound waves for secure device pairing and configuration. This addresses the specific issue of secure initialization in IoT devices, a problem that remains insufficiently addressed in existing solutions. The absence of similar approaches in the search results reinforces the originality and inventive nature of our proposed method.

10. Do you feel that a person of "average" skill (not-extraordinary skill) in your area of technology would have arrived at your invention with existing knowledge in public domain? If no, what could be the reasons for the same?

No, a person of average skill in the field of IoT technology would not have arrived at this invention using existing public domain knowledge.

Reasons:

1. **Integration of Inaudible Acoustic Signals**: The use of inaudible acoustic waves for secure initialization is a novel concept, requiring a deep understanding of sound wave manipulation, IoT communication protocols, and device pairing mechanisms, which goes beyond basic knowledge in the domain.

2. **Dynamic Hierarchy-Based Encryption**: Developing a system that adapts encryption levels dynamically based on device criticality and network roles

demands advanced expertise in cryptography and network security, areas not typically mastered by an average professional.

3. **Zero Trust Implementation in IoT**: Applying zero trust principles in an IoT-specific context involves innovative thinking and familiarity with cutting-edge security frameworks, which are not commonly accessible to those with general skill levels.

4. **Multidisciplinary Approach**: The invention spans multiple disciplines, including acoustics, cryptography, IoT device architecture, and energy optimization. Combining these fields effectively requires specialized knowledge and cross-domain expertise that an average skilled individual may lack.

Considering these factors, it is evident that a person with standard expertise in the field would not have devised our invention using publicly accessible knowledge. The novel integration of these elements in an innovative way distinguishes our solution and underscores its non-obvious nature.

11. Kindly provide broad workable ranges for all the parameters involved in your invention.

S.No	Parameters	Description	Workable Ranges	Comments
1.	**Acoustic Frequency**	Frequency determined dynamically based on the node to hub distance	Variable; computed under deployment	Optimized in real time to ensure effective propagation and minimal interference
2.	**Acoustic Signal Intensity**	Sound pressure level of the emitted initialization signal	Variable; computed under deployment	Adjustable to overcome ambient noise and maintain reliable communication
4.	**Node-to-Hub distance**	Maximum effective range for acoustic signal transmission	0.5 m – 10 m	Dependent on environmental conditions and device sensitivity

5.	**Initialization Time**	Time required to complete the secure acoustic initialization process	0.5 sec – 5 sec	Influenced by signal processing speed and network congestion
6.	**Data Rate for Acoustic Transmission**	Speed at which initialization data is transmitted acoustically	1 kbps – 100 kbps	Adequate for key exchange and transmission of initial parameters
7.	**Encryption Key Length**	Size of cryptographic keys used during dynamic encryption	128-bit – 256-bit	Chosen based on the required security level for the network or the device
8.	**Encryption Hierarchy Levels**	Number of distinct encryption tiers for device categorization	1 – 5 levels	Provides tailored security by assigning stronger encryption to more critical nodes (5 being the most critical level and 0 being zero encryption open level)
9.	**Authentication Refresh Interval**	Frequency for re-authentication under the zero-trust framework	1 sec – 60 sec	Configurable according to risk tolerance and dynamic network conditions
10.	**Operating Temperature Range**	Environmental conditions within which devices operate reliably	-20°C – 60°C	Ensures stable functionality across diverse climatic conditions
11.	**Power Consumption During Initialization**	Energy required during the acoustic initialization phase	10mW– 50mW	Power consumption during initialization is highly dependent on the distance between the node and hub. As acoustic waves of greater power need to be emitted to avoid dissipation of signals before reaching node.

12. References

1. Kumar V, Malik N, Singla J,Jhanjhi NZ, Amsaad F, Razaque A. Light Weight Authentication Scheme for Smart Home IoT Devices. *Cryptography*. 2022; 6(3):37. https://doi.org/10.3390/cryptography6030037
2. Li, S., Iqbal, M. & Saxena, N. Future Industry Internet of Things with Zero-trust Security. *Inf Syst Front* **26**, 1653–1666 (2024). https://doi.org/10.1007/s10796-021-10199-5
3. Malik Qasaimeh, Raad S. Al-Qassas, Fida Mohammad, Shadi Aljawarneh, A Novel Simplified AES Algorithm for Lightweight Real-Time Applications: Testing and Discussion, Recent Advances in Computer Science and Communications; Volume 13, Issue 3, Year 2020, . DOI: 10.2174/2213275912666181214152207
4. Shenoy D, Patil A, Pandey AK. Revisiting Zero-Trust Security for Internet of Things. ResearchGate. https://www.researchgate.net/publication/377021858_Revisiting_Zero-Trust_Security_for_Internet_of_Things. Published 2023.
5. Smith T, Gomez J, Nguyen H. Theory and Application of Zero Trust Security: A Brief Survey. PMC. https://pmc.ncbi.nlm.nih.gov/articles/PMC10742574/. Published 2024.
6. Wang L, Zhou Q. Power IoT Security Protection Architecture Based on Zero Trust. IEEE Xplore. https://ieeexplore.ieee.org/document/9357607/. Published 2022.
7. Roy P, Mehta S, Khanna R. Zero Trust Real-Time Lightweight Access Control Protocol for Mobile Cloud-Based IoT Sensors. arXiv. https://arxiv.org/abs/2309.01293. Published 2024.
8. Kumar S, Patel V. ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Implementation. ACM Digital Library. https://dl.acm.org/doi/10.1145/3671147. Published 2023.
9. Acoustic Internet of Things Information Transmission System, Relay Base Station, and Method, Google Patents, 2018. [Online]. Available: https://patents.google.com/patent/SG11201810568QA/en.
10. Y. Ding, C. Wang, W. Chen, and F. Hu, "Ubiquitous acoustic sensing on commodity IoT devices: A survey," *ResearchGate*, 2022. [Online]. Available: https://www.researchgate.net/publication/357987192_Ubiquitous_Acoustic_Sensing_on_Commodity_IoT_Devices_A_Survey.

13. Inventors Details (Full Names, Nationality and Addresses)

Inventors Name	Nationality	Address
1. Manikandan S	Indian	**Vellore Institute of Technology, Chennai.**

14. Applicant Details (Full Names, Nationality and Addresses)

Applicant Name	**Nationality**	**Address**
Manikandan S (23BCE1476)	Indian	**Vellore Institute of Technology, Chennai.**

15. Any additional notes or remarks.

Nil

16. For Life Sciences related inventions:

i. **Provide source and geographical origin of the biological material/resource (for e.g. plants, animals, micro-organisms, their parts / genetic material and by-products with actual or potential use or value)**

Nil

ii. **Please note, if the biological material used in the invention is from India, then an application to seek approval of the National Biodiversity Authority(NBA) for applying for intellectual property rights (including patents) in or outside India needs to be made as per the Biological Diversity Act, 2002.**

Nil

iii. **Please indicate in case you need assistance to make an application to the NBA.**

No

Please provide sequence listing in computer readable format.

iv. **In case you would like us to prepare the sequence listing for submission to the Patent Office please indicate**

No

v. **Please indicate if the invention relates to novel biological material for example, bacteria, fungi, eukaryotic cell lines, plant spores, genetic vectors (such as plasmids or bacteriophage vectors or viruses) containing a gene or DNA fragments, or organisms used for expression of a gene (making the protein from the DNA).**

No

vi. **If Yes, have you deposited material with the recognized depositary under the Budapest Treaty?**

No

(Please note, in case of novel material as mentioned above, deposition must be made before filing of the patent application).