ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152

www.ijmece .com

Vol 12, Issue.2 April 2024

Untraceable and Unclonable Sensor Movement in the Distributed IoT Environment

Batti Pruthviraj [1], Bhukya Shalini Sumathi [2], Gaddam Praneeth Kumar [3], J Sai Kumar4,
Dr. K. Niranjan Reddy[5]
[1,2,3,4] UG Student, Department of ECE, CMR Institute of Technology, Hyderabad
[4] Associate Professor, Department of ECE,
CMR Institute of Technology, Hyderabad

Abstract

This article proposed a new protocol “untraceable and unclonable sensor movement in the distributed IoT environment”. The proposal has the following several advantages: (1) the new protocol using PUF achieved the main contributions of both untraceable and unclonable sensors. (2) the new protocol also achieved standard security features such as mutual authentication, perfect forward and backward secrecy. (3) The proposed authentication protocol can withstand from various kinds of attacks, such as to reply, DoS, impersonation, and cloning attack. (4) Analysis formally using BAN Logic has been conducted and denoted that the protocol achieved a secure mutual authentication. In addition, analysis formally using the RoR model and Scyther tool denoted that the proposed protocol withstands from various attacks. (5) A comparison of security features and computational complexity ensures that the proposal is secure and has low computational complexity.

Introduction

THE distributed IoT environment is an IoT environment consisting of several WSNs; connectivity between WSN and IoT device which can provide remote access and heterogeneous device communication. Several companies have utilized the distributed IoT environments, such as [1] IBM with Smart Planet, which utilizes a sensor as a primary component applied in a smart water management system and smart city. The other project is the HP lab with Central Nervous System for the Earth (CeNSE) by utilizing a sensor as a primary component. On the other hand, by utilizing 6LowPAN, it can integrate the components of WNS, such as sensor with web services of SOAP and REST [2], [3], and the other communication services, such as WhatsApp, Line, email, blogs, etc. [4], [5]. However, many challenges must be carefully considered. One of the challenges is related to the security and privacy problem. For example, senor movement in the distributed IoT-based healthcare system -, in which the patients with the body sensor network want to move from one room to the other room or from one hospital building to the others for treatments by keeping the patients' privacy. While the patients' body sensor can prove their legitimacy, their movements should remain secret for the security reasons. Several security features must be fulfilled to securelyprovide WSN as part of the IoT environment [6]. However, this paper focuses on untraceable and unclonable sensor movement. This proposal also considers achieving the standards of security features, such as mutual authentication, perfect forward and backward secrecy, and withstanding from various kinds of attacks including reply, DoS, and other attacks. Moreover, this paper also uses lightweight cryptography, such as XOR-operation and One-way-hashfunction. In addition, PUF is used to achieve a non-cloning device.

Literature survey

D. Guinard, M. Fischer, and V. Trifa, "Sharing Using Social Networks in a Composable Web of Things," 2010 8th IEEE Int. Conf. Pervasive Comput. Commun. Work. (PERCOM Work., pp. 702–707, 2010.

Exploiting things or sensors of smart phones with Apps has offered powerful personal services today. How do we extend this paradigm to network connected things or Internet of Things (IoT) to provide personal services is currently an important issue. Out of many platforms, Social Web of Thing (SWoT) has been considered a great platform for future App development because it integrates IoT and Social Networks (SN) and makes human readily monitor and manage smart objects. This work discusses technical options and various requirements of SWoT and presents a scalable and flexible MULtimedia-supported SWoT platform called MUL-SWoT. In particular, the platform provides easy integration of smart objects and 3rd party service providers. Additionally, it is capable of processing and handling multimedia data. We also describe a home monitoring and intrusion detection system that is built on the MUL-SWoT platform. A prototype of the platform is also implemented to illustrate the feasibility of our design. Internet of Things (IoT) [1] is a promising paradigm that aims to build a global network of heterogeneous, uniquely identifiable smart objects, sensors, and actuators. IoT enables us to collect ambient information and use this information in a wide range of applications adopted in many different domains, including intelligent transportation, logistics, environmental monitoring, surveillance, safety protection, etc

D. Mandl et al., "Sensor Web 2 . 0 : Connecting Earth' s Sensors via the Internet," no. January, 2008.

Sensors are everywhere, which includes space, air and ground. Earth phenomena such as disasters also occur everywhere; such as wildfires, floods and volcanoes. There is a need to rapidly deploy existing sensors to aid emergency workers and investigators. The vision for our effort is to provide users the capability to create "mash ups" (a web application that combines data from more than one source into an integrated experience), similar to that used by Google Earth users to create a composite map with overlays of sensor information and from other data sources such as weather, traffic, urban construction etc. We make use of Web 2.0 technology and Open Geospatial Consortium (OGC) Sensor Web Enablement (SWE) web service standards to enable access to Earth's sensors is an emerging mega-trend which will lower the cost of producing customized science by an order of magnitude. This paper will outline the key aspects of our experiments to date and implications for the future and in particular the Global Earth Observation System of Systems (GEOSS) international effort.

C. P. Mayer, "Security and Privacy Challenges in the Internet of Things," Electron. Commun. EASST Work. der Wissenschaftlichen Konf. Kommun. Verteilten Syst. 2009 (WowKiVS 2009), no. January 2009, 2013.

The future Internet of Things as an intelligent collaboration of miniaturized sensors poses new challenges to security and end-user privacy. The ITU has identified that the protection of data and privacy of users is one of the key challenges in the Internet of Things [Int05]: lack of confidence about privacy will result in decreased adoption among users and therefore is one of the driving factors in the success of the Internet of Things. This paper gives an overview, categorization, and analysis of security and privacy challenges in the Internet of Things. The Internet has undergone severe changes since its first launch in the late 1960s as an outcome of the ARPANET. The initial four-node network has quickly grown into a highly interconnected and self-organized network that builds the daily basis for business, research, and economy. The number of people using this worldwide network has exponentially grown up to about 1.5 bn and hereby makes up about 20% of the world population.

R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

In the Internet of Things, services can be provisioned using centralized architectures, where central entities acquire, process, and provide information. Alternatively, distributed architectures, where entities at the edge of the network exchange information and collaborate with each other in a dynamic way, can also be used. In order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages – not only in terms of features but also in terms of security and privacy challenges. The purpose of this paper is to show that the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths. The concept of the Internet of Things (IoT) has evolved over time [1, 2, 3]. Nevertheless, its core idea can be summarized in a sentence: ‘A worldwide network of interconnected entities’. In most cases, these heterogeneous entities, ‘things’ (e.g. Human beings and computers, books and cars, appliances and food) have a locatable, addressable, and readable counterpart on the Internet.

Existing system

The concept of untraceable and unclonable sensor movement in the distributed Internet of Things (IoT) environment introduces a novel approach to enhance the security and privacy of sensor data in interconnected systems. In the existing system, sensors are equipped with advanced technologies that make their movements and data transmission untraceable and unclonable. This is achieved through the integration of secure communication protocols, cryptographic techniques, and decentralized architectures.

The untraceable aspect ensures that the movement and location of sensors remain confidential. Traditional tracking methods, such as GPS or centralized monitoring systems, are mitigated, reducing the risk of unauthorized entities gaining insights into the physical whereabouts of sensors. This is particularly crucial in scenarios where sensitive data, such as surveillance or industrial information, is being collected.

Simultaneously, the unclonable nature of sensor movements ensures that each sensor in the distributed IoT environment is uniquely identified and resistant to cloning attempts. This is achieved through the incorporation of hardware-based security features, such as physically unclonable functions (PUFs) or secure elements. These technologies create a unique and unreproducible signature for each sensor, making it challenging for malicious actors to replicate or impersonate the devices.

The distributed nature of this system further enhances security by reducing the reliance on a single point of failure. Data transmission between sensors and the central system is often encrypted and decentralized, mitigating the risk of interception and tampering. Additionally, the use of blockchain or similar distributed ledger technologies can contribute to ensuring the integrity and immutability of sensor data.

This untraceable and unclonable sensor movement paradigm is particularly relevant in critical applications such as healthcare, industrial IoT, and surveillance, where maintaining the confidentiality and integrity of sensor data is of paramount importance. By incorporating these advanced security measures, the system provides a robust defense against potential threats in the increasingly interconnected landscape of the Internet of Things.

Proposed system

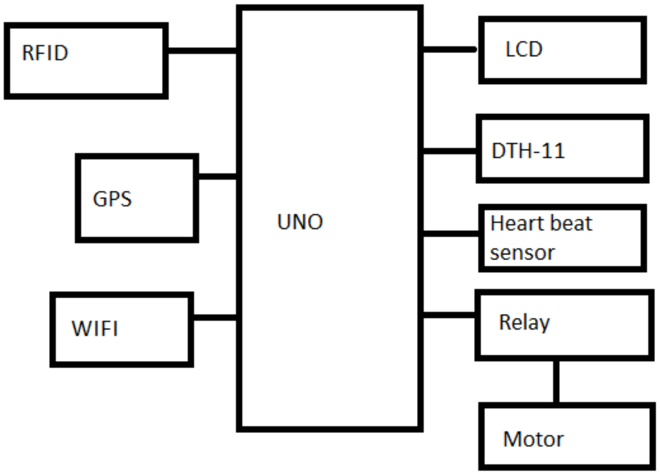
The proposed system for Untraceable and Unclonable Sensor Movement in the Distributed IoT Environment presents a groundbreaking approach to bolstering security and privacy in the Internet of Things (IoT) landscape. In a distributed IoT environment where sensors play a pivotal role in collecting and transmitting data, the system introduces advanced techniques to ensure the untraceability and unclonability of sensor movement.

Central to this system is the integration of cryptographic protocols and dynamic encryption algorithms applied to the communication between sensors. The use of these advanced encryption techniques ensures that the movement patterns of sensors remain obscured and untraceable to unauthorized entities. Additionally, the system employs unique identifiers and cryptographic keys for each sensor, making it practically impossible to clone or replicate sensor devices.

This untraceability and unclonability serve as a robust defense against potential security threats such as eavesdropping, unauthorized access, or malicious manipulation of sensor data. The dynamic nature of the encryption keys and the cryptographic protocols involved enhance the resilience of the system against sophisticated cyber attacks, providing a high level of security in the distributed IoT environment.

Moreover, the proposed system incorporates decentralized authentication mechanisms, reducing the reliance on a centralized authority for sensor verification. By distributing authentication processes across the IoT network, the system adds an extra layer of security, making it challenging for adversaries to compromise the entire system by targeting a single point of authentication.

The implementation of this system aligns with the growing concerns about privacy and security in the IoT landscape. As sensors become ubiquitous in various applications, ensuring the confidentiality and integrity of the data they generate is of paramount importance. The proposed system not only addresses these concerns but also contributes to the establishment of trust and reliability in distributed IoT environments by safeguarding sensor movement against traceability and cloning.**Block diagram**



HARDWARE COMPONENTS

LCD (Liquid Cristal Display)

Introduction:

A liquid crystal display (LCD) is a thin, flat display device made up of any number of color or monochrome pixels arrayed in front of a light source or reflector. Each pixel consists of a column of liquid crystal molecules suspended between two transparent electrodes, and two polarizing filters, the axes of polarity of which are perpendicular to each other. Without the liquid crystals between them, light passing through one would be blocked by the other. The liquid crystal twists the polarization of light entering one filter to allow it to pass through the other.

A program must interact with the outside world using input and output devices that communicate directly with a human being. One of the most common devices attached to an controller is an LCD display. Some of the most common LCDs connected to the contollers are 16X1, 16x2 and 20x2 displays. This means 16 characters per line by 1 line 16 characters per line by 2 lines and 20 characters per line by 2 lines, respectively.

RELAY MODULE

Relay modules are simply circuit boards that house one or more relays. They come in a variety of shapes and sizes, but are most commonly rectangular with 2, 4, or 8 relays mounted on them, sometimes even up to a 16 relays.

Relay modules contain other components than the relay unit. These include indicator LEDs, protection diodes, transistors, resistors, and other parts. But what is the module relay, which makes the bulk of the device? You may ask. Here are facts to note about it:

- A relay is an electrical switch that can be used to control devices and systems that use higher voltages. In the case of module relay, the mechanism is typically an electromagnet.
- The relay module input voltage is usually DC. However, the electrical load that a relay will control can be either AC or DC, but essentially within the limit levels that the relay is designed for.
- A relay module is available in an array of input voltage ratings: It can be a 3.2V or 5V relay module for low power switching, or it can be a 12 or 24V relay module for heavy-duty systems.
- The relay module information is normally printed on the surface of the device for ready reference. This includes the input voltage rating, switch voltage, and current limit.

Relay Module Function

What does a relay module do? The relay module function is mainly to switch electrical devices and systems on or off. It also serves to isolate the control circuit from the device or system being controlled.

This is important because it allows you the use a microcontroller or other low-power device to control devices with much higher voltages and currents.

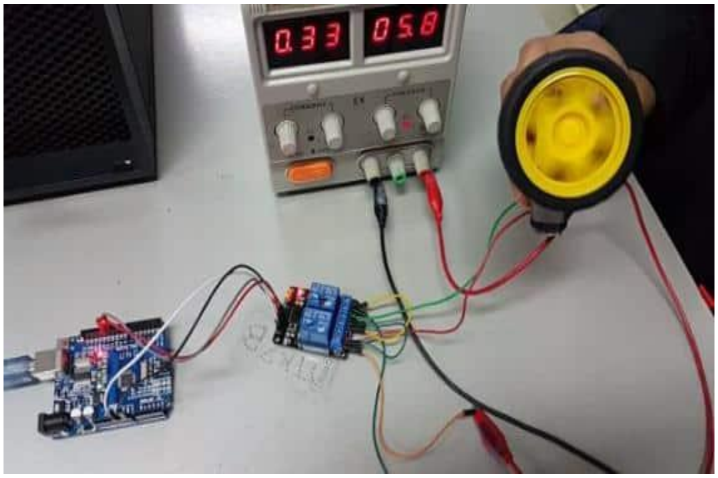
Another relay module purpose is to amplify the control signal so that it can switch the higher currents using only a small out of power from a microcontroller.

Relay Module vs. Relay

It is also important to note the difference between a relay vs. relay module. A relay is a single device that has an electromagnet and a switch, or it can be the solid-state type.

A relay module, on the other hand, is a board that has one or multiple relays on it and several other components to provide isolation and protection.

Because of its modular construction, this type of switching and control device can be many different configurations. It can be a single-channel relay module for a single load or it can be a multi-channel device with multiple relays to control several circuits.



Relay motor working demonstrated

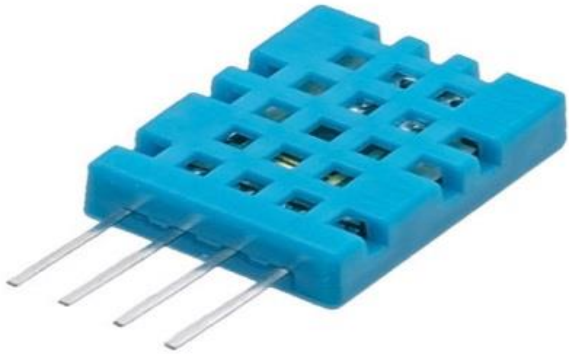
ESP8266

The ESP8266 is a low-cost Wi-Fi microchip, with a full TCP/IP stack and microcontroller capability, produced by EspressifSystems[1] in Shanghai, China. The chip first came to the attention of Western makers in August 2014 with the ESP-01 module, made by a third-party manufacturer Ai-Thinker. This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands. However, at first there was almost no English-language documentation on the chip and the commands it accepted.[2] The very low price and the fact that there were very few external components on the module, which suggested that it could eventually be very inexpensive in volume, attracted many hackers to explore the module, the chip, and the software on it, as well as to translate the Chinese documentation.[3] The ESP8285 is an ESP8266 with 1 MiB of built-in flash, allowing the building of single-chip devices capable of connecting to Wi-Fi.[4] The successors to these microcontroller chips is the ESP32 family of chips, including the pin-compatible ESP32-C3.

DHT TEMPERATURE & HUMIDITY SENSORS.

These sensors are very basic and slow, but are great for hobbyists who want to do some basic data logging. The DHT sensors are made of two parts, a capacitive humidity sensor and a thermistor. There is also a very basic chip inside that does some analog to digital conversion and spits out a digital signal with the temperature and humidity. The digital signal is fairly easy to read using any microcontroller.

Humidity is the measure of water vapour present in the air. The level of humidity in air affects various physical, chemical and biological processes. In industrial applications, humidity can affect the business cost of the products, health and safety of the employees. So, in semiconductor industries and control system industries measurement of humidity is very important. Humidity measurement determines the amount of moisture present in the gas that can be a mixture of water vapour, nitrogen, argon or pure gas etc… Humidity sensors are of two types based on their measurement units. They are a relative humidity sensor and Absolute humidity sensor. DHT11 is a digital temperature and humidity sensor.



DHT11 Sensor

DHT11 sensor has four pins- VCC, GND, Data Pin and a not connected pin. A pull-up resistor of 5k to 10k ohms is provided for communication between sensor and micro-controller.

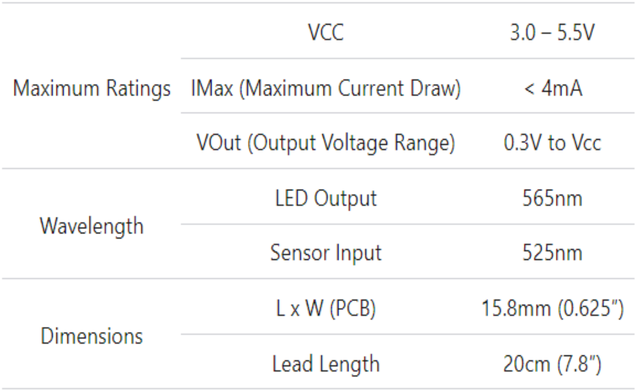
Applications

This sensor is used in various applications such as measuring humidity and temperature values in heating, ventilation and air conditioning systems. Weather stations also use these sensors to predict weather conditions. The humidity sensor is used as a preventive measure in homes where people are affected by humidity. Offices, cars, museums, greenhouses and industries use this sensor for measuring humidity values and as a safety measure.

It's compact size and sampling rate made this sensor popular among hobbyists. Some of the sensors which can be used as an alternative to DHT11 sensor are DHT22, AM2302, SHT71.

Heart beat

The front of the sensor, with the heart logo, is where you put your finger. You'll also notice a tiny circular opening through which the Kingbright's reverse mounted green LED shines.



Maximum Ratings	VCC	3.0 – 5.5V
	IMax (Maximum Current Draw)	< 4mA
	VOut (Output Voltage Range)	0.3V to Vcc
Wavelength	LED Output	565nm
	Sensor Input	525nm
Dimensions	L x W (PCB)	15.8mm (0.625")
	Lead Length	20cm (7.8")

Just beneath the circular opening is a small ambient light photo sensor – APDS-9008 from Avago. This sensor is similar to the ones used in cell phones, tablets, and laptops to adjust the screen's brightness based on the ambient lighting conditions.

Conclusion

This article proposes a new protocol by preserving the untraceable and unclonable sensor movement using stable-PUF to improve the security features and resolve the distributed IoT environment problems. Based on the informal analysis, our proposed scheme has fulfilled the security features, such as Mutual Authentication, Untracebility, Anonymity, and protection against impersonation attacks, as well as protected from the cloning attacks (SF1-SF5). In addition, the formal analysis using

BAN Logic ensures our scheme achieves the secure mutual authentication. The result of ROR model and Scyther tool show that our proposed scheme withstands from various kinds of attacks as well as proves and strengthens our informal analysis. On the other hand, based on the computational complexity comparison, our protocol obtains a lower computational cost than the schemes proposed by [15] and [19]. Therefore, our scheme is more suitable to be applied in the distributed IoT environment.

References

[1] IBM, "IBM builds a smarter planet." [Online]. Available: https://www.ibm.com/smarterplanet/us/en/.

[2] G. Montenegro, N. Kushalnagar, H. J, and C. D, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks Status," RFC4944, pp. 1–30, 2007.

[3] D. Guinard, M. Fischer, and V. Trifa, "Sharing Using Social Networks in a Composable Web of Things," 2010 8th IEEE Int. Conf. Pervasive Comput. Commun. Work. (PERCOM Work., pp. 702–707, 2010.

[4] Libelium, "Interfacing the Sensor Nateworks With the Web 2.0." [Online]. Available: https://www.libelium.com/.

[5] D. Mandl et al., "Sensor Web 2 . 0 : Connecting Earth' s Sensors via the Internet," no. January, 2008.

[6]C. P. Mayer, “Security and Privacy Challenges in the Internet of Things,” Electron. Commun. EASST Work. der Wissenschaftlichen Konf. Kommun. Verteilten Syst. 2009 (WowKiVS 2009), no. January 2009, 2013.

[7] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[8] F. Zhu, M. W. Mutka, and L. M. Ni, "Private Entity Authentication for Pervasive Computing Environments," Int. J. Netw. Secur., vol. 14, no. 2, pp. 86–100, 2012.

[9] S. Shin, T. Shon, H. Yeh, and K. Kim, "An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment," Peer-to-Peer Netw. Appl., vol. 7, pp. 612–619, 2014.

[10] P. Gope and T. Hwang, "Untraceable Sensor Movement in Distributed IoT Infrastructure," IEEE Sens. J., vol. 15, no. 9, pp. 5340–5348, 2015.

[11] Reddy, Kallem Niranjan, and Pappu Venkata Yasoda Jayasree. "Low Power Strain and Dimension Aware SRAM Cell

Design Using a New Tunnel FET and Domino Independent Logic." International Journal of Intelligent Engineering & Systems 11, no. 4 (2018).

[12] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Design of a Dual Doping Less Double Gate Tfet and Its Material Optimization Analysis on a 6t Sram Cells."

[13] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Low power process, voltage, and temperature (PVT) variations aware improved tunnel FET on 6T SRAM cells." Sustainable Computing: Informatics and Systems 21 (2019): 143-153.

[14] Reddy, K. Niranjan, and P. V. Y. Jayasree. "Survey on improvement of PVT aware variations in tunnel FET on SRAM cells." In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), pp. 703-705. IEEE, 2017

[15] Karne, R. K. ., & Sreeja, T. K. . (2023). PMLC- Predictions of Mobility and Transmission in a Lane-Based Cluster VANET Validated on Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5s), 477–483. https://doi.org/10.17762/ijritcc.v11i5s.7109

[16] Radha Krishna Karne and Dr. T. K. Sreeja (2022), A Novel Approach for Dynamic Stable Clustering in VANET Using Deep Learning (LSTM) Model. IJEER 10(4), 1092-1098. DOI: 10.37391/IJEER.100454.