Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

Create a Security Control System to Prevent Hackers from Tampering with IoT Devices

Saja Talib Ahmed[1], Dhahir Abdulhade Abdullah[2]

Abstract

With the expansion of the use of Internet of Things using Internet technology to control and operate highly confidential systems in areas of life and with government facilities such as hospitals or banks, they require high security for their system in both software and hardware to prevent theft by unauthorized persons, and only authorized persons can enter the system. Our proposed work includes an authentication system to enter the Internet of Things system. Where SoC is used to generate True Random Numbers. These numbers are used to reconnect the pins of the devices. Where the encryption of the random code is changed every time an attempt is made to enter the system by unauthorized persons by entering the password and username incorrectly, using SoC (4 Cortex-M chip) by generating a new code instead of changing the connection of the logical controllers. The random numbers are unpredictable, unique and cannot be predicted. TRNs were tested using NIST tests, and they achieved high results. The test results of these numbers also showed that they are unpredictable, unique, have a high entropy value per bit (0.999) and have no correlation with the value (-0.12333). Which means that reconnecting the pins to operate the devices is a difficult process to predict because it depends on numbers generated physically, not mathematically, and cannot be predicted.

Keywords: *Physical Unclonable Function (PUF), internet of things (IoT), True Random Numbers (TRNs), System on Chip (SoC).*

Introduction

The Internet of Things technology, which is used in many fields, uses heterogeneous devices and collects heterogeneous data, exposes the system to theft by unauthorized persons. To avoid this situation [1], a security system must be created for the Internet of Things system to prevent unauthorized persons from entering the system and not tampering with the system's data and devices, making it highly secure. This importance is due to the fact that IoT is used in important systems with sensitive data [2]. The use of IoT usually exposes the system to continuous hacking attacks due to its connection to the Internet. There are two reasons why IoT systems cannot use the Internet's current security protocols and approaches [3], [4]. Firstly, there is the underlying presumption that the nodes on the IoT platforms do not provide infinite power or memory. Secondly, devices with internet connectivity are thought to have strong physical security. Consequently, one of the main concerns with IoT devices is their physical security [5]. PUF phenomenon can be used as a technique to generate true random numbers [6]. In our proposed system TRNs will be generated using SoC to avoid network breach and entry into IoT system. Security measures will be implemented in two stages: hardware and software. When an initial breach of the system is detected, random codes will be generated (the SW stage), and based on these codes, the pins connections will be changed (the HW stage). These random numbers are unpredictable and pass all the NIST tests as shown in subsection (6.2), it has high Entropy as shown in subsection (6.3), and has low correlation as shown in subsection (6.4). The pins are linked based on these true random numbers. Therefore, hackers cannot predict, re-link, or manipulate them.

Related Work

Two PUF-based authentication algorithms for Internet of Things (IoT) systems were proposed in [7] by Aman et al. (2017). Despite this, their plan is not able to protect the privacy of IoT devices. Since every IoT device in the proposed protocol has a PUF, the system cost is high. when it is attempted to separate the PUF from the embedded system, the PUF will be destroyed.

[1] Department of Computer Science, College of Science, University of Diyala, Diyala, Iraq, scicomphd2206@uodiyala.edu.iq.
[2] Department of Computer Science, College of Science, University of Diyala, Diyala, Iraq, Dhahair@uodiyala.edu.iq.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

S. Banerjee et al. (2019) suggested in [8] to put in place a mechanism with a deadline for users to register, update their identification, and re-register. The higher power consumption of the IoT node might have an impact on its lifetime.

S. Sciancalepore et al. (2020) in [9] utilized the ECDH scheme and ECQV certificates. Because several messages are exchanged for key negotiation and authentication, they concentrated on the power consumption of IoT during authentication. Memory is required for the proposed system in addition to the sensitive data on the system.

All these related work can protect the IoT system as a software. If the hacker can get the password and username, or can hack the authentication system, he will be able to access the devices. There is no protection for the devices. But in our proposed system, if the hacker tries to get in for the first time, the SoC will disconnect the devices and generate random codes to reconnect the devices again (by an authorized user) so that only the authorized person can access them.

The Internet of Things

IoT Architecture

Three key parts make up the Internet of Things architecture: the user, cloud server, and IoT devices [10] (sensors, actuators, or any other type of communication device). IoT consists of three primary levels, each with a distinct function in the architecture, such as data sensing, data transmission, and data retrieval. The three main levels are [11]:

Perception layer

Network layer

Application layer.

They are the gadgets that capture information from their surroundings and send it via the Internet of Things gateway to cloud servers [12]. These devices have the ability to deliver a message from the sender to the recipient; it is possible for both the sender and the recipient to be IoT devices in this scenario fig. 1 in below shows these devices. A few well-known devices for the Internet of Things are [13]: Smart devices, Gateways, Sensors, Actuators, Servers, GSM.

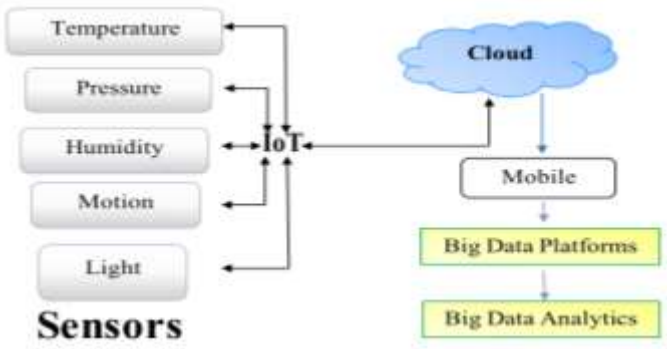

Fig. 1 IoT Architecture

Data collected from the environment can be stored on cloud servers. After the data from the IoT sensors or actuators is stored in the cloud, the end user is the last party to get the message, alert, or notice. For an

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

application to be considered valuable to the system, there must be no delay or deletion in the received data [14].

IoT Security

The implementation of IoT security architectures is heavily dependent on security. Strong defenses against intrusions are provided by the security. Application, protocol/functionality, and general specific are the three categories under which IoT-based security falls [15].

To provide secure end-to-end connectivity, real-time application-specific security monitoring systems use System-On-Chip, to ensure confidentiality, integrity and authenticity. [16].

Solutions for specific tasks like identity management, privacy enforcement, and service discovery are offered by the functionality-specific. By generating and eliminating the possibility of security assaults, the protocol-specific offers remedies for protocol weaknesses. This enables the policies to be implemented at the model level, enabling the analysis and development of distributed, varied, and communication protocols using both cloud programming and Internet of Things models [17].

As a result, while putting the IoT into implementation, security is a crucial issue that must be addressed. Below is a discussion of some IoT security areas [18]:

Confidentiality: is the greatest threat with the Internet of Things. Each device's data is kept private by confidentiality, which also prevents the device from sharing data with neighbors. Additionally, confidentiality may be used to conceal data from a passive intruder, ensuring the privacy of any messages delivered via sensor networks.

Integrity is the most important component of a communication network that end-to-end security protocols can capture. An integrity feature is needed to guarantee that data exchanged between various IoT devices is accurate and correct between the sender and the receiver.

During data transmission, no data tampering, loss, or alteration should occur. By utilizing security protocols and services, the information traffic is managed.

Accessibility: is the ability for the user to obtain information when various smart device kinds inside the network establish connections with one another.

Authentication: both the source and destination devices must be authenticated in order to guarantee that the information is only received by the authorized users.

Only authorized people are allowed access to this data thanks to authentication, which also allows different entities to interact and share accurate information.

Lightweight Solutions: When enabling security protocols and services, the power constraints of Internet of Things devices are taken into account. The security guidelines or practices are made to use less energy. The security method must work with devices that have security protocols as it will be implemented on end devices with specific, restricted capabilities.

Heterogeneity in the IoT system: is common as different devices can have different underlying hardware and software. IoT devices connected with each other can be from different vendors, can have different levels of complications, and can have different functionalities. So, in order to deal with these heterogeneous devices efficiently, the security protocol must be designed accordingly.

To enable communication between heterogeneous devices, the Internet of Things system requires a heterogeneous network. Because of this heterogeneity, the finest cryptography and security standards need to be used to ensure that there are no security breaches.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

Policies: Some standards and policies require that these policies and standards are implemented, which is very important, whether the devices are compliant with these rules or not. This allows information to be managed in a cost-effective and secure manner. Service Level Agreements have been introduced to deal with such circumstances.

Since the Internet of Things is made up of a variety of devices, consumers get a sense of confidence and trust as a result of these policies and processes [19].

Key Management Systems: These are necessary to protect the confidentiality of data between sensors and Internet of Things devices to build mutual trust among different parties.

System on Chip SoC and TRNG

System on Chip

A new generation of processors, the ARM Cortex family offers a standard architecture for a broad range of technological demands [20].

The Cortex family of CPUs, in contrast to other ARM CPUs, is a complete processing core that offers a standard CPU and system architecture [21]. There are three primary profiles for the Cortex family: A for high-end applications, R for real-time, and M for microcontroller and cost-sensitive applications. The Cortex-M4 profile, on which the STM32 is based, was created with excellent system performance and low power consumption in mind. It is not too costly to compete with conventional 8- and 16-bit microcontrollers [22]. STMicroelectronics combines the Arm Cortex-M4 core with its unique licensed low-power silicon intellectual property, hardware accelerators, non-volatile embedded memory technology, and other components to create the STM32 Arm Cortex-M4 MCUs, high-performance designs, and knowledge of wireless networking [23]. Fig. 2 shows the STM32 Cortex-M4 for Control and performance for mixed signal devices. The Cortex-M4 microcontrollers are completely integrated into the STM32 Cube development environment and utilize the resources and tools provided by ST's extensive network of partners [24].

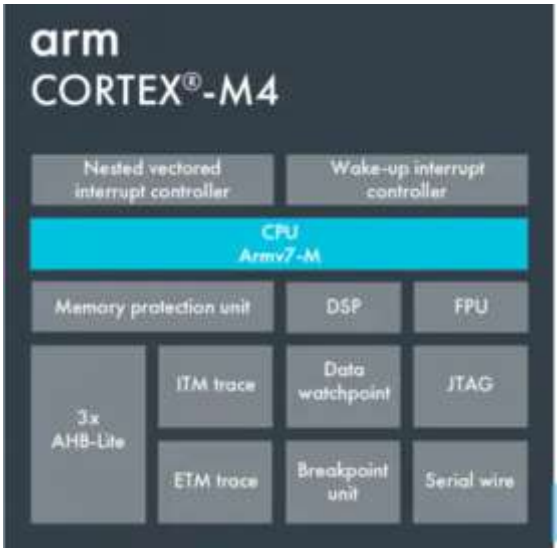

Figure 2: Arm Cortex-M4 Block Diagram [24]

TRNG using Arbiter PUF

For the Internet of Things (IoT), randomness is a major problem. Because of the cryptographic protocols, there is a requirement to produce random numbers that are appropriate for Internet of Things devices with

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

limited resources and size [25]. Among the most popular methods for producing TRN are PUF-arbiter circuits [26].

Delay-based PUFs of this kind generate their response bit by comparing the delays of two delay paths that are nominally identical but have slightly varied delays as a result of variances in the manufacturing process. A basic explanation of this type is given in Fig. 3. An arbiter PUF's paths connect to a decision-making arbiter block, which functions as a phase comparator in essence, as follows [27]:

a. If path 1 is faster, the first state generates a 1.

b. If path 2 is faster, the second state generates a 0.

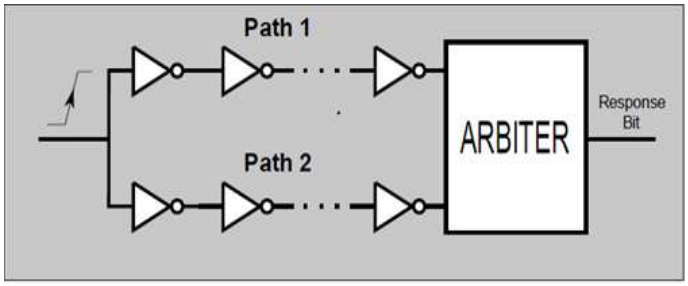

Fig. 3. Simplified Arbiter PUF [27]

In Figure 2.7, an edge is introduced, two paths are put in competition, and the top signal is ultimately sampled by the bottom signal. The faster (or slower) of the two paths is then indicated by a binary value produced by the arbiter circuit. There is not much of a delay difference between the two parallel paths because they are similar [28].

The proposed system

Flowchart of the proposed system

The proposed system is clarified in fig. 4.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

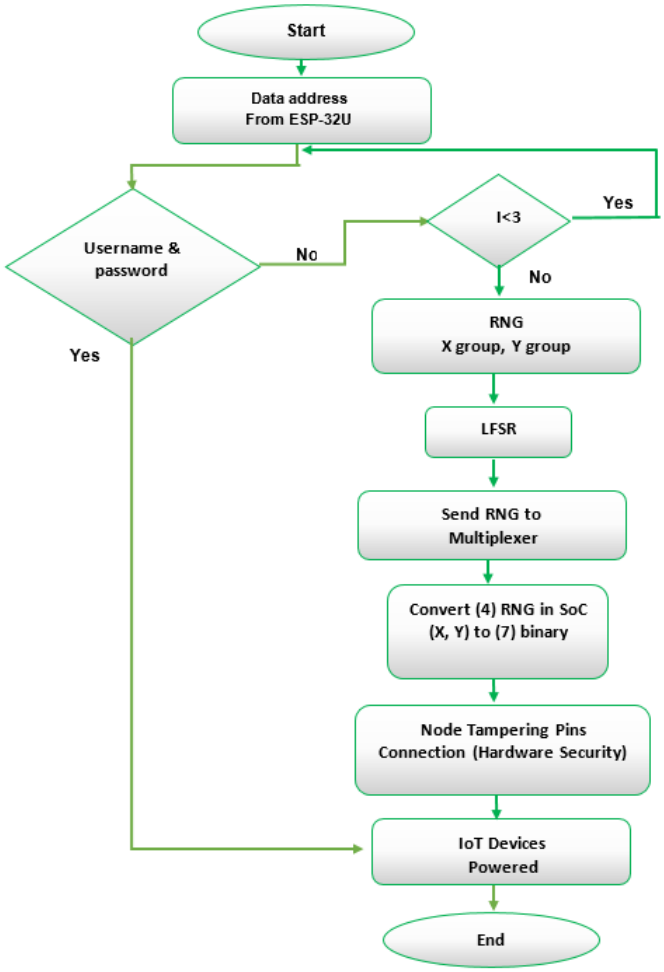

Fig. 4: SoC of the proposed system

In proposed work, the SoC is programmed, if the wireless system is hacked for three possible insertions of the user and password (as shown in previous paper), the wireless shield begins by giving an alert that the IoT system will be closed by using the SoC by starting to generate a random number code. The process is considered to change the system from IoT to an encrypted system as shown in fig. 5., and fig. 6.

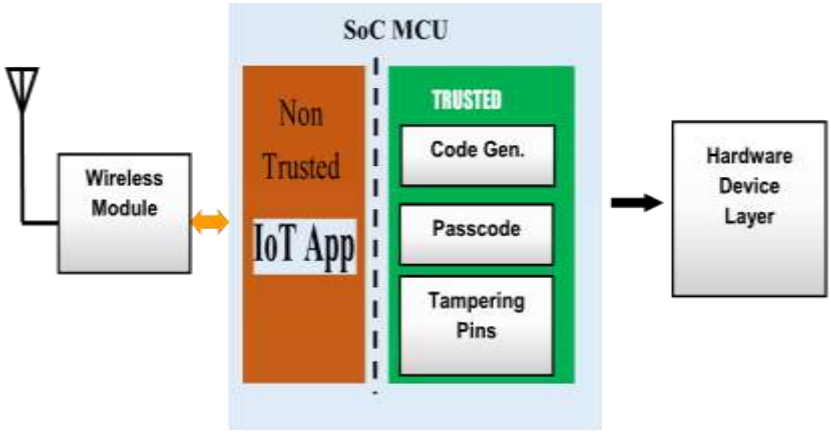

Fig. 5. IoT Node Security

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

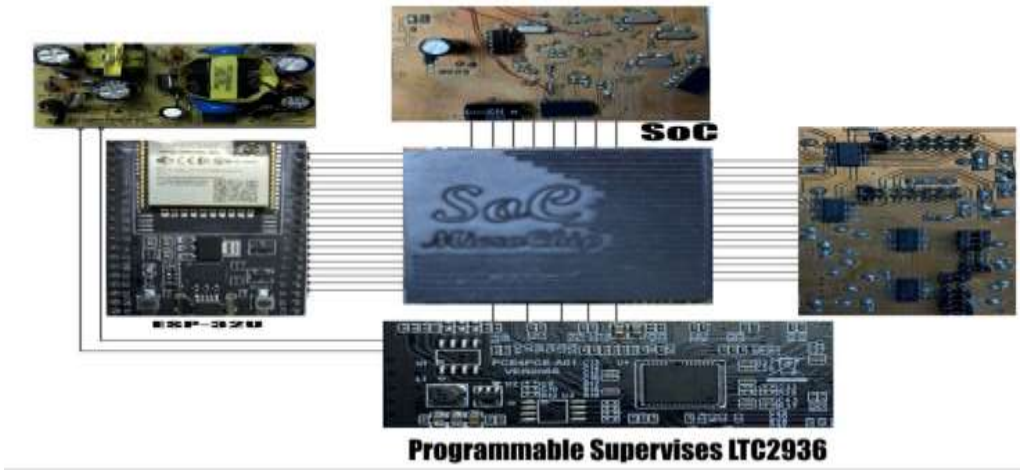

Fig. 6. SoC Circuit Security of IoT

When the user input false username and password, the SoC begins to construct a (4) randomness bit of the (X) group and (Y) group for each device of IoT for (4) devices totally (X4) and (Y4) every time when insert the wrong username and password of the IoT web page that sending address data change, which lead to the SoC the (X) and (Y) group generated new one this in turn is sent to the entrance of multiplexer digital circuit, which represent the hardware security circuit of IoT. When sending the four-bit encrypted code, SoC performs mathematical operation groups for the purpose of generating random numbers. These random numbers are in two groups with (4) bits for each group.

Then these random numbers are sent to the LFSR to increase the security by making some confusion, then the output are sent to the input of the digital integrated circuits (multiplexers) for the purpose of converting each group of X and Y into (7) bits and then into the hardware security stage (node tampering circuits), which are in the form of logical circuits (pull-up and pull-down) input logic and that (14) bits for each device of the IoT system. By sum these codes of two groups (X, Y) become (14) bits, these bits match a communication system between the outputs of the multiplexer and the optic-coupler, this is shown in fig. 7.

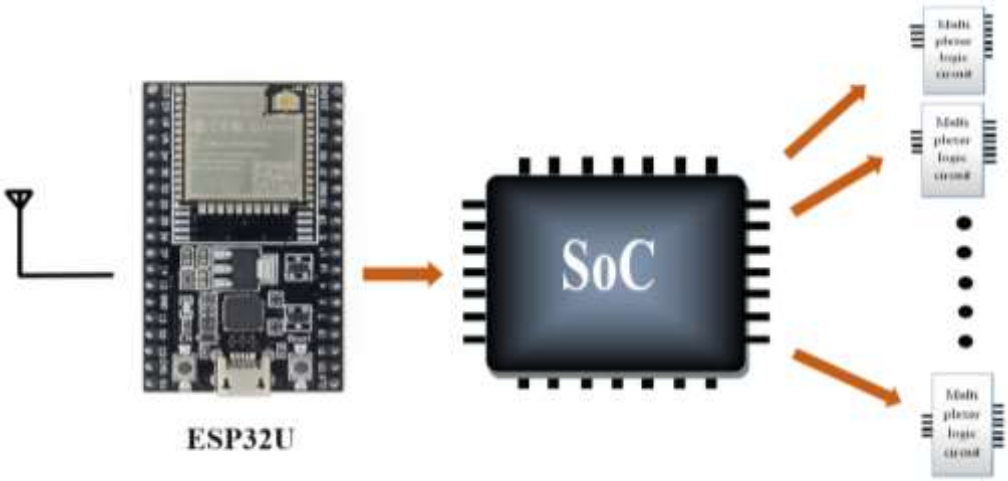

Fig. 7. SoC Interface with Tampering Circuits Pins

This is for two parts of the positive pole, which represents the set of (X), and the negative pole, which represents the set of (Y). Then the relay for that device is fed to deliver what, is required for the IoT system. It is worth noting that it is possible to expand the work of the system to more than (40) devices.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

The system keeps all the devices associated with it until they enter the IoT system again to change the state of the devices. With the SoC cortex-M4 core, it is possible to program for the security of IoT systems with a wide range of different random numbers, meaning it is possible to obtain high security for the IoT with a large capacity of random numbers.

Tampering Circuits

Tampering circuits are a serious issue in the IoT. The IoT devices are used to collect environmental circuits (hardware security). In our proposed system the tampering circuit is used for IoT to protect all data after the SoC generates random numbers to input into the logic circuit device, which are multiplexed to seven binary code numbers as shown in fig. 8. The connection can change according to the encrypted codes.

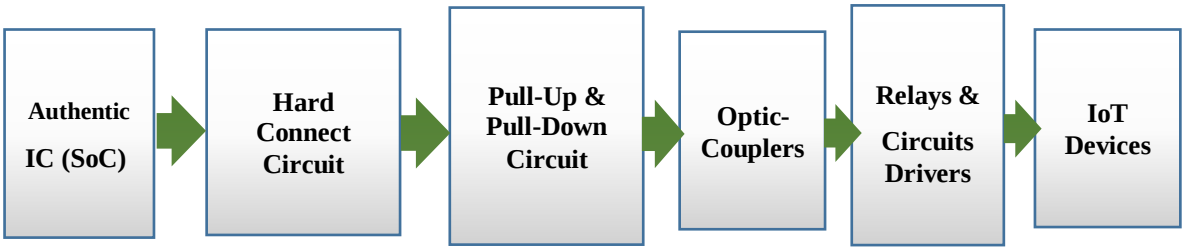

Fig.8. Node tampering hardware circuit of IoT

The connection is changed to the section of the circuit, after which the node tampering process is done to feed the device, which is controlled with IoT. Fig. 9. shows the authentication process of the Physical Unclonable Function (PUF) using the SoC.

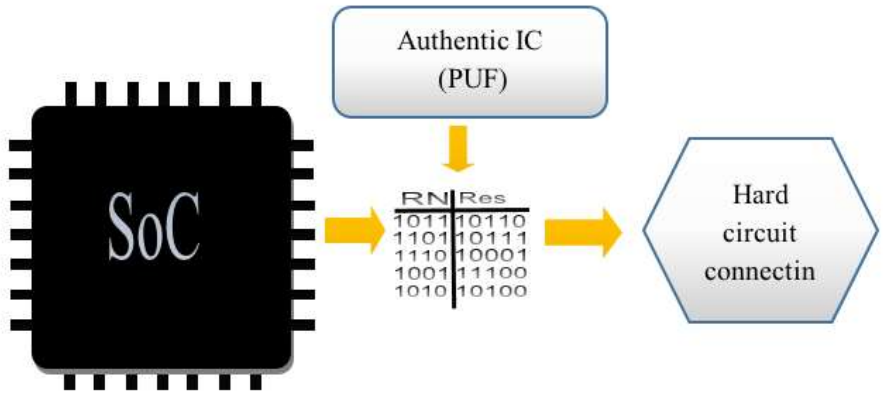

Fig. 9. The Physical Unclonable Function (PUF) authentication process employs (SoC).

Fig.10. shows the parts of a hard circuit logic with a changeable pins connection between this circuit and the Pull-Up and Pull-Down circuits to operate the IoT devices. Depending on the truth table of the multiplexer logic circuit.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

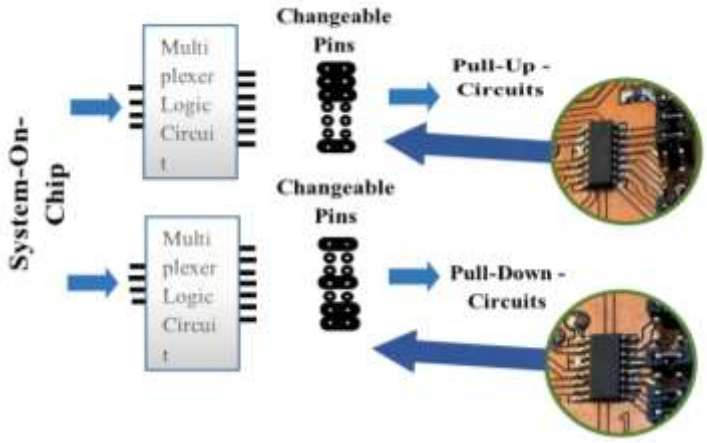

Fig.10 Multiplexer Hard Connection Circuit with a changeable Pins Connection

Pull-Up and Pull-Down Circuits

The output of each of the twice-logic circuit drives is a Pull-Up circuit, and the other is Pull-Down input circuit.

After setting the connection pins according to the code encryption truth table, each circuit powers the optic-couplers to drive the circuits of the relays in the IoT system. Any disagreement between the output of the logic circuit that is given code-generating by (SoC) and the array pin connections leads to unsuccessful to drive the relays of the internet of things.

Relays Driver Circuits

The last circuits, which connect between the optic-couplers and drivers' circuits to drive the relays of the internet of things separately for each encryption code and for each driver, have two outputs, Pull-Up and Pull-Down, which are controlled by the (14) encryption code (7) bits for Pull-Up and (7) for Pull-Down circuits. Each (4)-bit input pin is under the truth table of the (1)-set connection. The circuit shown in fig.11. the circuit driving two poles of one relay for one device of the IoT.

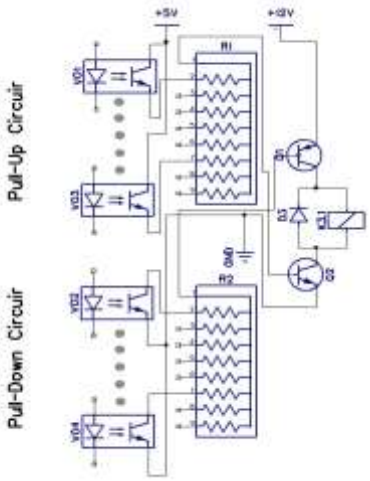

Fig.11. Relays Driver Circuit

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

Results and Evaluation

This section is presenting the results and the assessments that evaluate the performance of the proposed system. Different measurements are used to evaluate the proposed system, which are the SoC Authentication phase, and the Node Tampering phase.

Tests of TRNG

True random numbers, which are generated by the SoC as previously described in subsection (3.2), are used in the authentication phase. Table 1 shows (15) physical numbers in binary form (the length of the numbers, number of bits, can be changed).

Table 1: Samples of (64) Hardware Random Numbers for X and Y groups

	X	Y
1	1011	1010
2	0111	0101
3	1110	1010
4	1100	0100
5	1001	1001
6	0010	0010
7	0100	1111
8	1001	1011
9	1010	0110
10	0001	0011
11	0011	0111
12	0101	1000
13	0110	1100
14	1000	1101
15	1111	1110

After the TRN is generated, the LFSR algorithm will be used to increase security and add some confusion, and then the output will be sent to the multiplexer HCF4511, which will expand the bits from 4 bits to 7 bits for both groups X and Y, making them 14 bits. Table 2. shows the code encryption which is the result of these processes.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

Table 2: Code Encryption

Pull-Up circuit Code	Pull-Down circuit Code
1111000	0000111
1011100	0100011
1001110	0110001
1000111	0111000
0111100	1000011
0101110	1010001
0100111	1011000
0011110	1100001

NIST Test for randomization

In order to assess a cryptographic system's security, one of the most important steps is to test the sequence of random numbers. different tests are given in subsections (6.2.2), (6.2.3).

In this section, NIST tests will be used. The results for the 12 tests are shown in Table 3.

Table 3: P-value and Lowest Proportion of passed Tests

Test-name	***outcomes***	***P.Value >0.01***	***The lowest rate of success***
FFT Test	Pass	0.43223	100%
Rank Test	Pass	0.39324	100%
Non-periodic Templates Test	Pass	0.999999	82%
Frequency Test	Pass	0.343233	99%
Approximate Entropy test	Pass	1	100%
Overlapping Template of all One's Test	Pass	1	100%
Lempel-Ziv compression Test	Pass	1	100%
Runs Test	Pass	0.54345	98%
Longest Run of One's test	Pass	1	100%
Block Frequency Test	Pass	0.948984	100%
Serial Test	Pass	0.527521	98%

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

Cumulative Sums Test (Forward)	Pass	0.582332	100%

Evaluation the results of the Entropy Test

This test calculates the Entropy of the numbers. Table 4. shows the results of the entropy test performed on the bits produced by the SoC (2496126) bits.

Table 4. The result of Entropy

No. Bits	P(1)	P(0)	Log (1)	Log (0)	Entropy value
2496126	1247999	1248127	6.0962142374	6.0962587781	0.9999926938

The random numbers generated by Arbiter, shown in Table 4, have high entropy (0.9999); this means that these circuits generate unpredictable random numbers. True Random Numbers (TRNs).

Evaluation the results of the correlation test

The results of the correlation test performed on the bits produced by the SoC (2496126) bits are shown in Table 5 There is a negative correlation, when the correlation is less than 0 it means there is no correlation.

Table 5. The result of Correlation

No. Bits	C 11	C 10	C 01	C 00	Correlation value
2496126	413766	566333	564232	412698	-0.155388483

That means the random numbers that generated by the PUF are True random numbers.

The Results of Tampering Circuits

The tampering nodes and their connections are explained in subsection (5.2), where the hardware security of the IoT system is achieved. Figure 4.2 shows that the pins are connected according to the generated random numbers. These connections are changed whenever the attackers try to break into the system, after three attempts to enter the system the system is locked and the connections of these pins are changed. Therefore, no unauthorized person can access the system and tamper with the devices and data, unless he reconnects the pins of each device. This is called physical tamper protection of devices.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

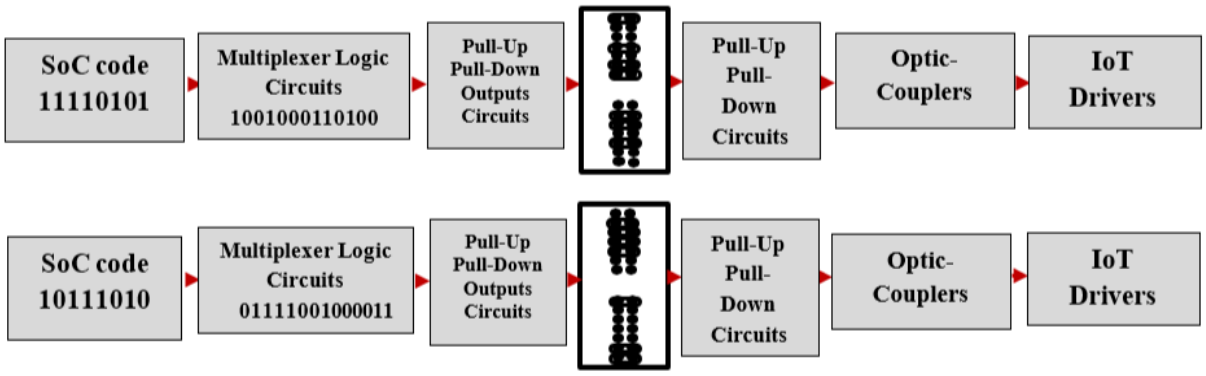

Fig.12: Approach Tampering Pins for tow Samples Connections

Conclusion

Our proposed system is capable of providing authentication security. It achieves high software security and high hardware security with low hardware complexity. It is robust against modeling attacks because the proposed design modeling is nonlinear. The random numbers generated by the SoC are true random numbers because they do not depend on any mathematical function. They depend on interrupt events. Tables 3, 4, and 5 show that the numbers generated by the SoC are completely unpredictable, have no correlation, are high entropy, and do not require any initial inputs, which makes pin reconnection prediction very difficult, thus preventing access and tampering of devices. The proposed system does not require storing any important data inside the hardware components, so there is no sensitive data to be stolen. In addition, all the devices in the IoT use only one SoC, which reduces the cost and complexity of the system. The tamper-resistant pins of the node add more security to the devices.

References

[1] Chew, D. (2018). The Wireless Internet of Things: A Guide to the Lower Layers. John Wiley & Sons.
[2] Attkan, A., & Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex & Intelligent Systems, 8(4), 3559-3591.
[3] Security in the Internet of Things, Wind River, January 2015, http: //www.windriver.com/whitepapers/security-in-the-internet-of-things/ wr security-in-the-internet-of-things.pdf.
[4] G. Woo, P. Kheradpour, D. Shen and D. Katabi, "Gartner Says the Internet of Things Will Transform the Data Center," Gartner, March 2014.
[5] Sauer, F. (2021). Quantum technologies: Implications for security and defence.
[6] Acosta, A. J., Addabbo, T., & Tena-Sánchez, E. (2017). Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. International Journal of Circuit Theory and Applications, 45(2), 145-169.
[7] Aman, M. N., Chua, K. C., & Sikdar, B. (2017). Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 4(5), 1327-1340.
[8] Banerjee, S., Odelu, V., Das, A. K., Srinivas, J., Kumar, N., Chattopadhyay, S., & Choo, K. K. R. (2019). A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment. IEEE Internet of Things Journal, 6(5), 8739-8752.
[9] Sciancalepore, S., Piro, G., Boggia, G., & Bianchi, G. (2020). Public key authentication and key agreement in IoT devices with minimal airtime consumption. IEEE Embedded Systems Letters, 9(1), 1-4.
[10] Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The internet of things (iot): An overview. International Journal of Engineering Research and Applications, 5(12), 71-82.
[11] Wu, C. K., & Wu. (2021). Internet of Things Security. Springer Singapore.
[12] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future generation computer systems, 56, 684-700.
[13] Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.
[14] Perry, L. (2020). IOT and Edge Computing for architects: Implementing edge and IOT systems from sensors to clouds with communication systems, analytics and Security. Packt.
[15] Abughazaleh, N., Bin, R., & Btish, M. (2020). DoS attacks in IoT systems and proposed solutions. Int. J. Comput. Appl, 176(33), 16-19.

Journal of Ecohumanism
2024
Volume: 3, No: 8, pp. 339 – 352
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i8.4737

[16] Ghatikar, G. (2017). Internet of things and smart grid standardization. Internet of Things and Data Analytics Handbook, 495-512.
[17] Herrero, R. (2022). Fundamentals of IoT communication technologies. Cham: Springer.
[18] Alioto, M. (Ed.). (2017). Enabling the internet of things: From integrated circuits to integrated systems. Springer.
[19] Raj, P., Poongodi, T., Balusamy, B., & Khari, M. (Eds.). (2020). The internet of things and big data analytics: integrated platforms and industry use cases. CRC Press.
[20] Lucan Orăşan, I., Seiculescu, C., & Căleanu, C. D. (2022). A brief review of deep neural network implementations for ARM cortex-M processor. Electronics, 11(16), 2545.
[21] Iturbe, X., Venu, B., Ozer, E., Poupat, J. L., Gimenez, G., & Zurek, H. U. (2019). The Arm triple core lock-step (TCLS) processor. ACM Transactions on Computer Systems (TOCS), 36(3), 1-30.
[22] Halak, B. (2012). Authentication of Embedded Devices. University of Southampton, UK. ISBN 978-3-030-60768-5 ISBN 978-3-030-60769-2 (eBook) https://doi.org/10.1007/978-3-030-60769-2 © Springer Nature Switzerland AG 2021.
[23] Xiao, P. (2018). Designing Embedded Systems and the Internet of Things (IoT) with the ARM mbed. John Wiley & Sons.
[24] Spanulescu, S. (2021). ARM Microcontrollers Programming for Embedded Systems. Everand, Ebooks: 9780463529751.
[25] Seyhan, K., & Akleylek, S. (2022). Classification of random number generator applications in IoT: A comprehensive taxonomy. Journal of Information Security and Applications, 71, 103365.
[26] Kimbro, C., Gordon, H., & Lyp, T. (2021). Telehealth Sensor Authentication Through Memory Chip Variability.
[27] O'donnell, C. W., Suh, G. E., & Devadas, S. (2004). PUF-based random number generation. MIT CSAIL CSG Technical Memo, 481.
[28] O'CONNOR, M. I., VERBAUWHEDE, M. I., ROUZEYRE, M. B., & FISCHER, M. V. (2014). Modélisation et Caractérisation des Fonctions non Clonables Physiquement (Doctoral dissertation, Orange Labs).