Secured Water Quality Monitoring System based on IOT

Ahmed Abbas Fadel¹, Mohamed Ibrahim Shujaa²
Middle Technical University (MTU), Electrical Engineering Technical College, Baghdad

Abstract. Nowadays, the Internet of Things is used in many areas and applications such as smart cities and smart houses. However, the widespread Internet of things (IOT) faces many problems, the most important of those which are related to confidence and privacy. Information security is the main challenge on the Internet of things. To gain a secure and good quality of water, a smart monitoring and secured process system was introduced. In this paper the present algorithm was used to transmit information safely and secure, after the generation of the random key of the algorithm. Sensors was used to sense the change in reading parameters of the acidic/basic water (PH) ,and total dissolved solids ( TDS) of water, then transfer information from the external environment to the proposed system where the microprocessor (ESP32) and website application. The achieved results showed that the encryption method on the PH and TDS readings parameters succeeds in maintaining the avalanche effect requirement and introducing additional strength to the system.

Keyword: IoT, Ph, TDS, Security, chaotic.

1. Introduction

Internet of Things (IoT) is a rapid technology that enables things “devices” to communicate and share information between them without human control it is used in many different aspects of life. Such as industrial, agricultural, sports and military fields .The widespread of IoT has simplified the everyday life activities, In IoT, security is divided into two parts, first, the security of the communication network which require to secure the network from any intruder device which can send or receive information in the network, hence an authentication and authorization mechanism is required. Second, the information itself should be secure also by means of encryption techniques [1, 2] An advanced water monitoring system was used which depends on measuring water parameters such as water level and turbidity. The network detention of IOT is very wide and consists of a set of physical elements. These sets of the network can get an ample offset challenges in improving applications[3]. Security is one of the challenges faced by systems that depend on the Internet of Things because the devices used are the non-high specification and have facilitated penetration by attackers who usually target data sent between the main control devices and data centers, and by directly attacking attackers for that data, they may violate the main security principles are Confidentiality, Integrity, and Authentication [4].

Despite the widespread of the Internet of things, it faces many security problems [5], to reduce these problems; many researchers have proposed solutions to these security problems. It has been suggested [6] to use a lightweight algorithm , the SIMON algorithm was used after improving its performance.
In [7] it was suggested to use the DES and RSA to encode the data when transferring, and a simulation was performed using MATLAB. In recent years, Blockchain has good massive attention due to its major features including immutability, suitability, and security, resulting from these major features, blockchain has been applied in multiple applications like the Internet of Things (IoT). However, blockchain is highly expensive. In [8] proposed of an (LSB) hat is improved for IoT needs while also providing rise security. Some symmetric and asymmetric encryption algorithms such as BLOWFISH, RSA, DES [9]. These algorithms prevent unauthorized access to sensitive data in the period of collection or delivery to the next layer. It is recommended to apply these algorithms to this layer as it consumes little energy.

2. Related Work

- **P. Nandhini and V. Vanitha, 2017** [10]. Proposed a new compact hybrid lightweight encryption technique using fastest bit permutation instruction PERMS with S-box of PRESENT.

- **Mustafa et al., 2019** [11]. Proposed a modified AES algorithm with Lightweight issue, in this proposal the Mix Columns operation combined with add round key operation to perform in one cycle, the shift-row operation was modified to shift-rows and shift-columns and finally the number of rounds was reduced to 6 rounds only. The proposed algorithm passed the statistical tests and was faster than standard AES, which made it applicable for IoT resources.

- **Choi, Jongsoek et al., 2018** [12]. Created the practical necessities in the IoT data security sharing system, so as to substantiate the functions to be performed between the individuals within the reference model of the IoT data security sharing system.

- **BODEI, Chiara; et al., 2019** [13]. Suggested present a strategy, supported the method calculus IoT-Lysa, to infer quantitative measures on the evolution of systems. The derived quantitative analysis is exploited to ascertain the price of the potential security countermeasures, in terms of time and energy.

- **Nesa, Nashreen, and Indrajit Banerjee, 2020** [14]. Suggested a security protocol that involves each authentication of deployed IoT devices and encryption of generated knowledge. The planned algorithmic rule involves cryptologic operations that incur a really low process price needs comparatively little storage and at the identical time are highly resilient to security attacks.

- **N. Sklavos and I. D. Zaharakis, 2016** [15]. Their work focused on hardware implementation efficiency, communications confidentiality, user authentication, data integrity, and service availability. They also conceded modern attacks, threats, and countermeasures against them. For general purpose usages were offered such scheme: for ensuring confidentiality, they used Advanced Encryption Standard (AES), an asymmetric algorithm (RSA) and Digital signatures - for key management. As an alternative to RSA can be applied Diffie-Hellman (DH) and Elliptic Curve Cryptography (ECC).

3. Hardware and Software Requirements:

Hardware and software are critical specifications to be addressed when developing the proposed program. Hardware and software specifications can be described as:

1- Laptop or Smartphone.
2- Microsoft Visual studio.
3- Microsoft SQL server.
4- Python.
5- ESP32 Microcontroller.
6- Sensors.
4. Proposed Architectural Design and Development:

The Internet of Things Applications is one of the technologies that have grown in the present area and there are many applications like smart home applications, smart hotels, and smart water stations. [16] Smart water stations are considered to be one of the important applications for measuring and monitoring the quality of water in rivers and water stations, where they exhibit sensitivities at different locations of rivers and water stations, and through these sensors, which read the changes of the PH and T.D.S of water and are securely sent to the website located in the control center. The main components used in developing the proposed system are classified into three main layers, and each layer contains the set of operations, as follows:
1- Application layer: This layer includes a set of related user and web operations.
2- Security Layer: All security related operations will be explained in this layer.
3- Physical Layer: This layer includes the structure used to connect ESP32 with sensors.

4.1. Hybrid Key Generation for lightweight algorithms

Due to the randomness features of the output from chaotic systems, all needed tools in this work are constructed using chaotic systems, and the construction of each tool dependent on other tools to give better security. Two chaotic systems are used in the construction of a secret key generation. In this work we need many stages, The first stage is to construct random bits generator using 2D Henon map chaotic, then in the second stage, we use the output from the Cat map also as the output of a random bit. For more secure we designed this hybrid generator by applying a swap operation between x, y output in Henon and Cat maps for viable attackers, This process is illustrated in Figure (1), which are used to construct a secret key generator for the present algorithm. After the swapping operation is done, we must merge between the left and right sides, finally, the XOR operation is processed. This step is repeated until it generates all keys.

![Figure (1): Secret Key Proposal Structure with Present Algorithm.](image)

Generating secure key algorithm based on Henon and Cat map chaos theory:

**Algorithm (1): Secret key generator from Henon and Cat map**
Input: initial and condition values

Output: secret key to Present

Begin

Step01: For $i = 1$ to 31 do

Step02: Get $X_i$ and $Y_i$ from Henone

Step03: Get $X_m$ and $Y_m$ from Cat

Step04: Concat between $X$ from Henon and $Y_m$ from Cat

Step05: Concat between $y$ from Henon and $X_m$ from Cat

Step06: Xoring between (4,5) steps to make the $K_i$ as secret key

Step07: If $K_i < 31$ then

Step08: $X_i = X_i + 1$

Step09: $Y_i = Y_i + 1$

Step10: $X_m = X_m + 1$

Step11: $Y_m = Y_m + 1$

Step12: Update Henon and Cat equation

Step13: End If

Step14: End For

End

4.2. Data transmission and secure Process:
The following figure illustrates the Confidentiality process of data transmission, and security.

![Confidentiality process](image)

Figure (2): Confidentiality process.

4.3. Physical Layer and Water Monitoring System Architecture
The proposed water monitoring for the IoT system contains three steps, figure (3) shows the block diagram of the proposed IoT system for water tests as case study. The first step in the IoT system is the sensing data collection from sensors connected to the IoT control. In this work, we have two types of sensors used in collecting data from water. These sensors are (TDS) and (pH meter) these sensors are connected with the microcontroller (ESP32) in the second stage, in (ESP32) control the collection data is encryption based on the Present algorithm. In the third step after all encrypted information is sent to a special web application,
it can decrypt or store information in the web. The proposed work is described as shown in figure (3).

Figure (3). Block diagram of the proposed system.

5. Result and Discussion
Framework for Registration Approval is the main services provided in the web application suggested as shown in figure (4). This process is managed professionally by the administrator. There are two actors, user, and admin in this process. When the user is registered with the Workflow user will see the applications that require your support, approval service. This procedure cannot be done until the central administrator approves and supplies the Identification code allowing authentication to be accomplished. This proposed water efficiency system was presented in the improved electronic circuit. By considering the suitable value of PH, and TDS, we took samples of water from different places and regions, to find out the efficiency of this device in a different reading. As shown in Table (1). Results were displayed encrypted and decryption after being received by the web. However, the table shows the efficiency of the device as the results are very identical to the original results. To find out the efficiency of this device in a different reading value, these samples were taken to the Ministry of Technological Sciences for examination with specialized devices to prove the efficiency of the proposed device.
Table (1) shows a set of encrypted and decrypted values for (PH) and (TDS), respectively:

| TDS               | PH               |
|-------------------|------------------|
| Encrypted Value   | Decrypted Value  |
| 167254302323743   | 306              |
| 125768413721798   | 394              |
| 311307844502903   | 457              |
| 761423934462353   | 404              |
| 917091883405204   | 303              |
| 917091883405204   | 303              |
| 743199542916636   | 321              |
| 103069903635791   | 317              |
| 120420418873346   | 345              |
| 172746356613695   | 350              |
| Decrypted Value   | Encrypted Value  |
| 724327414834297   | 167254302323743  |
| 427710832405945   | 125768413721798  |
| 337010837658253   | 311307844502903  |
| 825375021738769   | 761423934462353  |
| 437361507865022   | 917091883405204  |
| 427710832405945   | 917091883405204  |
| 329703655389279   | 743199542916636  |
| 164560346320374   | 103069903635791  |
| 120030168341926   | 120420418873346  |
| 495048863106625   | 172746356613695  |
| Encrypted Value   | Decrypted Value  |
| 7.030626          | 167254302323743  |
| 7.024217          | 125768413721798  |
| 7.024929          | 311307844502903  |
| 7.018519          | 761423934462353  |
| 7.014245          | 917091883405204  |
| 7.019942          | 917091883405204  |
| 7.019942          | 743199542916636  |
| 7.009260          | 103069903635791  |
| 7.005698          | 120420418873346  |
| 7.035678          | 172746356613695  |

6. CONCLUSION

The complete design of advanced and smart monitoring and security system based on the Internet of things was introduced. The system consists of the microcontroller (ESP32), two type of sensors used in collecting data from water for measuring the PH and TDS. The implemented system performed accurate measures of PH, and TDS of the water. The measured parameters are sent from smart meter sensors to (ESP32) microcontroller, where it's secured and encrypted by the present algorithm and sent to the web application. The results showed that the change and different reading in the output of the PH and TDS fulfill the requirement of the security monitoring system. Our future work will focus on the implementation of the
proposed system in database systems which cover a large zone to gain different reading of PH and TDS.

7. Reference
1. Hussein, Noor A., and Mohamed Ibrahim Shuja. "DNA computing based stream cipher for internet of things using MQTT protocol." International Journal of Electrical & Computer Engineering (2088-8708) 10 (2020).
2. Casado-Vara, R., Novais, P., Gil, A. B., Prieto, J., & Corchado, J. M. (2019). Distributed continuous-time fault estimation control for multiple devices in IoT networks. *IEEE Access*, 7, 11972-11984.
3. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38, 8-27.
4. Neshenko, N., Bou-Harb, E., Chichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, 21(3), 2702-2733.
5. Garg, S., Kaur, K., Batra, S., Kaddoum, G., Kumar, N., & Boukerche, A. (2020). A multistage anomaly detection scheme for augmenting the security in IoT-enabled applications. *Future Generation Computer Systems*, 104, 105-118.
6. Alassaf, N., Gutub, A., Parah, S. A., & Al Ghamdi, M. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimedia Tools and Applications*, 78(23), 32633-32657.
7. Hussain, I., Negi, M. C., & Pandey, N. (2017, December). A secure IoT-based power plant control using RSA and DES encryption techniques in data link layer. In 2017 *International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS)* (pp. 464-470). IEEE.
8. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing*, 134, 180-197.
9. Kaur, J., Sharma, E. S., & Tech, M. (2018). Secure image sharing on cloud using cryptographic algorithms: survey. *International Journal on Future Revolution in Computer Science & Communication Engineering*, 4(2), 319-325.
10. P. Nandhini and V. Vanitha, "A Study of Lightweight Cryptographic Algorithms for IoT", International Journal of Computer Applications, ,vol. 6, no. 1, pp. 26–35, 2017.
11. M . Mustafa. Abd Zaid and Soukaena Hassan , ” Modification Advanced Encryption Standard for Design Lightweight Algorithms “, Journal of Kufa for Mathematics and Computer, Vol. 6, No. 1,Mar.,pp 21-27,2019.
12. Choi, J., Shin, Y., & Cho, S. (2018, January). Study on information security sharing system among the industrial IoT service and product provider. In 2018 *International Conference on Information Networking (ICOIN)* (pp. 551-555). IEEE.
13. Bodei, Chiara, Stefano Chessa, and Letterio Galletta. "Measuring security in IoT communications." *Theoretical Computer Science* 764 (2019): 100-124.
14. Nesa, Nashreen, and Indrajit Banerjee. "A Lightweight Security Protocol for IoT Using Merkle Hash Tree and Chaotic Cryptography." *Advanced Computing and Systems for Security*. Springer, Singapore, 2020. 3-16.
15. N. Sklavos and I. D. Zahirakis, “Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations,” 8th IFIP Int. Conf. New Technol. Mobil. Secur., pp. 1–2, 2016.
16. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*, 7, 82721-82743.