International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Combined Approach of Identity Based and Attribute Based Encryption Service to Secure Data Processing in WBAN

Manish Shrivastava[1*], Princy Matlani[2]

Submitted: 01/10/2023 **Revised:** 02/11/2023 **Accepted:** 12/11/2023

Abstract: Wireless Body Area Network (WBAN) is a collection of wireless sensor nodes that can be placed inside or outside the body of a human or living person to observe or monitor the functionality and adjacent situations of the body. By using a wireless body network, the patient becomes more physically versatile and is no longer forced to stay in the hospitals. Cloud computing is the next big thing after the Internet in WBAN. Even though cloud is becoming more popular, ease of use and respectability, privacy issues and other security issues is a big setback in the field of cloud computing. Privacy and security are the key factors for cloud storage. Encryption is a prominent technology for protecting sensitive data. In this paper, a combined approach of identity-based and attribute-based access policy for encryption (CAIBABE) of cloud storage is proposed, which can be implemented on a cloud platform. In this work, the feasibility of the encryption algorithm for data security and privacy in cloud storage is analyzed in comparison with other existing algorithms.

Keywords: *Cloud storage, cipher text, encryption, access control, attribute-based encryption, constant cipher text length, decryption, cryptography.*

INTRODUCTION

Based on data from the world population perspective [1] The 2017 revision projects that the population of older people elderly 60 or older will growth from 962 million in 2017 to 201 billion in 2050 and 3.1 billion in 2100. As older people belonging to this age group are uncovered to numerous kinds of health issues, they may need medical remedy more regularly to live within the world. therefore, it's miles inconvenient for them to tour lengthy distances from their domestic to the clinical Centre. Presently, in most regions of the sector with economically rising and lagging nations, conventional hospital therapy is maintained and these care Centre's display patients at positive times of the day or week. This type of diagnosis does not reduce the health problems of the patients. Therefore, a continuous patient monitoring system is needed to provide better treatment for this age group of patients.

Currently, wireless body area network (WBAN) is rising developments to permit real time and ongoing tracking in distinct regions, together with telemedicine. [2]The WBAN includes small size actuators and sensors. These sensor nodes are located either immediately on a patient's body or below the skin of the patient, to capture the bio-indicators like Electro cardio Gram (ECG), Elector Encephalon Gram(EEG), pressure and glucose level of Blood, movement of body and heart rate. These sensors are communicating wirelessly among themselves.

[1*]*Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, CG, India*
[2]*Department of Computer Science & Engineering, Guru Ghasidas University, Bilaspur, CG, India*

This kind of sensor network permits patients to be released early from medical middle and additionally viable to reveal their situations at home. although the patients are discharge from nursing home, their disease related information is to be had within the medical institution server. right here, the database inside the clinic need to be kept as secret as possible.

because the wireless body area network sensing gadgets are used to acquire sensitive information and may be in conflict conditions, they need a complicated and very secure medium or structure to keep away from the harmful verbal exchange in the gadget. These devices constitute numerous security and privacy measures for sensitive and personal patient medical facts. patient medical records location giant and unresolved scenario may additionally occur which may additionally result in alteration or exploitation of the system.

In this research paper, we first give an overview of WBAN as used for healthcare monitoring, their architecture, then highlight the major security and privacy requirements and attacks on different network layers in a WBAN and finally talk about (CAIBABE) cryptographic algorithms and laws that provide a solution for security and privacy in WBAN.

Related Works

R. Du et.al [3] proposes a Privacy-Preserving Searchable Encryption (PPSE) scheme based on public and private block chains. First, we save an encrypted index in a private block chain and offload the corresponding encrypted documents to a public block chain. The encrypted documents are found through the encrypted index. This method can reduce the storage overhead on the block chains and increase the efficiency of transaction execution and the security of

the stored data. In addition, we use a smart contract to introduce a secondary access control mechanism and restrict data users' access to the private block chain through authorization to ensure data privacy and access control correctness.

K. B et.al [4] Cloud computing provides the computer system resources such as data storage and computing power without client management by the user. The security protocols U-IDMP, Predicate Encryption, Functional Re-encryption, SAPA, Dynamic auditing protocol, Fully Homomorphic Encryption, PDP and PIR are analyzed for the vulnerabilities of cloud environment. The strength of these protocols in terms of privacy, integrity and authorization has been analyzed and the vulnerabilities have been identified.

Y. Yang et.al [5] introduce some random numbers and random permutation to enhance the security of ASPE scheme, and then propose a novel privacy-preserving Spatial Keyword Query (SKQ) scheme based on the improved ASPE and Geohash algorithm. Moreover, we design a Lightweight Spatial Keyword Query (LSKQ) scheme by using a unified spatial domain index and multiple keywords, which not only significantly reduces the storage and computational cost of SKQ, but also requires users to provide little information about the query region. Finally, a formal security analysis proves that our methods are indistinguishable under the Chosen Plaintext Attack (IND-CPA). Extensive experiments show that our improved method is efficient and practical.

X. Ma et.al [6] propose a novel server-side deduplication scheme for encrypted data in a hybrid cloud architecture, in which a public cloud (Pub- CSP) manages the storage and a private cloud (Pri- CSP) as the data owner handles the deduplication and dynamic ownership management. To reduce communication overhead, we use a first-uploader verification mechanism to make sure that only the first uploader needs to carry out encryption, and employ an get entry to control method that tests the validity of data users earlier than they down load information. Our safety evaluation and overall performance assessment display that our proposed server-side deduplication approach has higher performance in terms of security, effectiveness and practicality compared to preceding techniques. at the equal time, our method can successfully resist collusion attacks and forgery attacks.

Z. Li, et.al [7] propose a physical layer based security approach that uses the information of the physical channel and eliminates the additional hardware requirements. In particular, we investigate a group based cooperation to generate asymmetric secret key via the accumulation of Received Signal Strength Indicator (RSSI) data at the physical or link layer. We propose a practical cooperative group solution to increase the similarity, fluctuation and density of RSSI data for highly efficient key generation. The main innovation is to fully exploit multiple channels between a subscriber node and a group or between two groups to randomly synthesize RSSI data with multiple data densities and enhanced data similarity and fluctuation.

A. Nabila et.al [8] presents a comparative analysis of wireless standards IEEE 802.15.4 and IEEE 802.15.6 over a WBAN healthcare monitoring system based on sub-layer MAC. The main aim of this work is to look for certain factors to decide which standard provides the optimal quality of service (QoS) for such a system under normal traffic conditions. To this end, an extensive series of simulations were carried out using the Castalia simulator to evaluate the average latency, throughput and reliability of the two standards under the same conditions.

X. Yuan et.al [9] proposes a Two-Stage Potential Game based Computation Offloading Strategy (TPOS) to optimize resource allocation considering task and user priorities of WBANs. First we built a system utility maximization problem over the QoS of tasks. The reward, cost and penalty capabilities are given to model the shifting of computations. Then, we suggest a two-degree optimization technique to resolve the problem of mutual constraint strategies inside the method area of the ability game model, which reduces the computational complexity and improves the feasibility of the algorithm.

D. Yadav et.al [10] First, we start with the transmission round to select the cluster head. For this we need to define a criterion based on certain energy values for selecting a node as cluster head. In the cluster head selection phase, a probability distribution based on probabilistic clustering is used. In the transmission phase, members send their data to the cluster head and the cluster head forwards the collected data directly to the destination. As each packet is transmitted, a signature is appended to the transmitted data packets.

P. C. Paul et.al [11] WBAN-based healthcare applications collect health-related data, making them even more attractive to attackers. Ensuring the security and privacy of records in a WBAN application is certainly one of the most important challenges for an organisation. maximum developers have restrained knowledge of market-specific regulatory requirements and security requirements, and there are a massive quantity of security controls inside sufficient implementation details. This makes it hard for developers to enforce countermeasures to make sure security and privacy

The goal of this paper is to offer the methodology used to develop a data protection and privacy risk management framework for WBAN applications in healthcare. We also describe how the framework addresses the above demanding situations.

S. Ma et.al [12] introduce a new concept of public-key encryption with outsourced equality checking (PKE-OET) that can be adapted to cloud-based IoT environments and provides a flexible solution to protect against OMRA without introducing information about the entrusted parties into the encryption. We formally define the security model of PKE-OET against three types of attackers, including IND-CCA -I, IND-CCA-II and IND-CCA-III. We present a generic PKE-OET construction using a new variant of the smooth projective hash function (SPHF) with a novel lin-hom property that is of independent interest.

METHODOLOGY

The proposed work uses a heterogeneous encryption scheme that satisfies the following conditions: (1) The private key generator (PKG) and the key generation

centre (KGC) can generate different master keys and system parameters for different cryptography environments, which is more practical for heterogeneous systems.(2) The system is secure for both authenticity and confidentiality, and the formal definitions and security models for heterogeneous encryption systems are also given. (3) Each user maps to a unique pseudo-identity to achieve conditional identity preservation. A trusted entity can determine the real identity if needed. (4) Use encryption to implement a sender that encrypts its message once to the receiver.

Properties of proposed system

The proposed system contains four properties, namely a private key generator, a key generation centre, a sender IDA and n receivers, which enable IDA to send m messages to n receivers.

The private key generator and the key generation centre compute the pseudo identities for the users in the network along with the key pairs/private keys. We use a key extraction function in G1, which we call KEF.

Preliminary

In this section we describe bilinear maps and difficult problems. Let us consider two cyclic groups

G1and G2 with the same prime order q, and let P be a generator of G1.

A bilinear map Must satisfy the following properties:

1. Bilinearity : For all P, Q, , and e(P + R, Q) = e(P, Q)e(R, Q). Also e(aP, bQ) = e(P, Q)ab.
2. Non-degeneracy: There exists P, QG1, such that e(P, Q) 1.
3. Computability: e(P, Q) can be computed for P, Q G1.

Definition 1. Provided with the two groups G1 and G2 of the same prime order q, a bilinear map e: G1 × G1 ->G2, and a generator P of G1, the decision-dependent bilinear Diffie-Hellman problem is to decide whether T = $e(P, P)^{abc}$ for given (P, aP, bP, cP) and TG2.

Definition 2. Variants decision-dependent bilinear Diffie-Hellman problem is to decide whether T = e(P, P) abc−1 for given (P, aP, bP, cP, c−1P) and TG2.

Definition 3. Variants computational bilinear Diffie-Hellman problem is to compute T = e (P, P)abd−1for given (P, aP, bP, dP, d−1P).

Setup phase:

Setup: Let G1 and G2 be two cyclic groups of prime order q, where G1 is additive and G2 is multiplicative, and P is the generator of G1. Let e: be an admissible bilinear map, a key extract function KEF:, where is the length of the key.

1. Private Key generator randomly selects and two hash functions: computes, where a master secret key known only to the Private Key Generator.
2. Key generation center randomly choose and four hash functions: computes where s2 is a secret master key known only to the key generation center.

Identity-based cryptography: In identity-based cryptography, users obtain their private key as follows:

1. Sender A randomly choose and calculates $ID_{A,1}= k_A$ P and transmits (RID_A, $ID_{A,1}$) to Private Key generator, in which RID_A is the real identity of sender A. Private Key generator computes IDA,2= , where T denotes the valid period for the generated pseudo- identity. Eventually, the identity so sender A is
2. Private Key generator create a private key to the IBC users as, where as is sent to A through a secure path.

Encryption

A sender A encrypts n number of messages as to n receiver as follows:

1. Randomly choose, and calculate.
2. Calculate and let φ = (φ1, φ2,,φn).
3. Calculate C = DEM. Enc(K,M) where K=KDF(r2) and =(m ⊕R1||m2⊕R2||…||mn⊕ Rn).
4. Compute
5. Compute and let S = (S1, S2, ….., Sn).

Return cipher text

Decrypt: After receiving the cipher text the receiver Decrypts σ as follows:

1. Calculate and get.
2. Recover M = DEM. Dec(K,C) where. Receiver B, retrieve own message mi= (mi ⊕ Ri) ⊕ Ri.
3. Calculate
4. Accept with the message if and only if, following equation holds:

Proposed Access control scheme

The access control scheme consists of four phases : the initialization phase, the registration phase, authentication and authorization phase and the revocation phase.

Initialization Phase

In this phase, the SP executes the setup algorithm and manages a WBAN. The controller is assigned an identity IDB , a public key PKB and a private key SB. The private key can be handed over online or offline. If the online method is chosen, we can use a secure socket layer to ensure the confidentiality of the private key.

Registration Phase

A user has to register at SP to get the access permission to WBAN. The user first sends his identity IDA to SP, whereupon SP checks whether the identity is valid. If this identity is not valid, SP rejects the registration request. Otherwise, SP sets an expiry date ED and runs the Extract- Partial-Private-Key algorithm to generate a partial private key

Here, || is a concatenation symbol. The user can check whether the equation holds, the DA is valid

Otherwise, the DA is not valid. After obtaining DA, the user performs Generate-User-Key and Set-Private-Key to obtain a full private key SA and a public key PKA. The user publishes the public key without certification.

Authentication and Authorization Phase

If the user with the identity IDA wants to access the

monitoring data of the WBAN, it first generates a query message m [13]. To resist the replay attack and preserve anonymity, the user concatenates the query message, a timestamp TS, and the user's identity and public key into a new message. Then the user runs the algorithm Encrypt, which takes as input the new message m', the private key, the identity, and the public key of the user, and the identity and the public key of the controller, and outputs a σ = (c, S, T). Finally, the user sends the cipher text σ to the controller. When the controller receives the user's request, it first calculates and obtains. Then the controller calculates and checks whether holds. If the above equation does not apply, the request is rejected. Otherwise, the user is authorized to access the WBAN data. In this case, the controller encrypts the collected data using a symmetric cipher algorithm with the session key

RESULTS AND DISCUSSION

In this section, we evaluate our proposed system using performance metrics. We need to compare our mechanism with the existing system. This segment of paper has the research results based on PDR, throughput, packet loss, delay, energy consumption and routing overhead.

POCKET DELIVERY RATIO (PDR)

PDR compares the number of packets successfully received by the destination node (Rni) with thetotalnumberofpacketssentbythesourcenode(Sni).PD Risusedtomeasurethesuccessof the delivery rate. The higher the PDR value, the higher the network performance. PDR is one of the QoS parameters that indicates the success rate of a routing protocol and can be calculated as follows

$$PDR = \frac{\left(\sum_{i=0}^{N} Rn_i\right)}{\left(\sum_{i=0}^{N} Sn_i\right)}.$$

The PDR results of CAIBABE and the existing methods are shown in Figure 1. The PDR of IDE and DEEC has an average value of 95% and 98% respectively, while that of CAIBABE reaches 99%. This result shows that CAIBABE is better than IDE and DEEC in the moving node scenario.

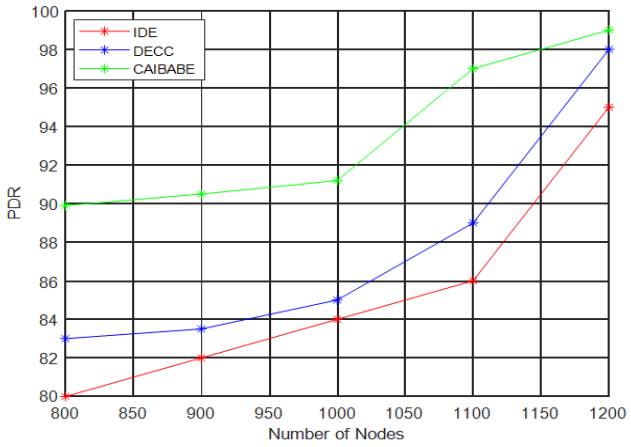

Fig 1 PDR comparison of proposed method with IDE and DEEC

Throughput

Throughput is the effective rate at which data is transmitted, while in this paper it is measured in bytes per second (Bps). Throughput is the total number of successful packets arriving at the destination device in a given time interval divided by the duration of the time interval. The most important aspect of throughput is the availability of sufficient bandwidth for the application .This determines the amount of traffic an application can receive as it traverses the network. This throughput can be measured after the data transmission has taken place and can be calculated with

$$\text{Throughput} = \frac{\text{total of the packet sent}}{\text{total data sending time}}.$$

The throughput result s of the CAIBABE and existing methods are shown as in Figure2.
The figure represents that the default CAIBABE has a higher throughput value than IDE and DEEC.

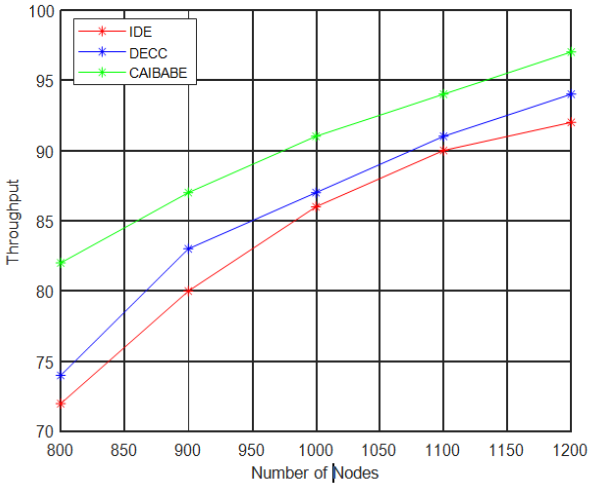

Fig 2 Throughput comparison

Packet Loss

The percentage of packets lost is the total number of packets sent over the network in relation to time.IntheTCPprotocol,whenapacketlossoccurs,thelostpacketisretransmitted,resultingin increased overhead in the form of wasted energy to forward a lost packet. The UDP protocol, on the other hand, does not resend a lost packet, resulting in packet loss. There are several causes of packet loss on the network, such as network congestion, damage to the packet, errors in the physical media and failure of the receiver to transmit (i.e. buffer overload). Packet loss can be calculated with

$$\text{Packet Loss} = \frac{\text{total of packet sent} - \text{total of the packet received}}{\text{total of packet sent}}.$$

Packet loss remains the same for DEEC and CAIBABE up to 10 to 30 nodes, but with the increasing number of nodes packet loss also increasing for CAIBABE.

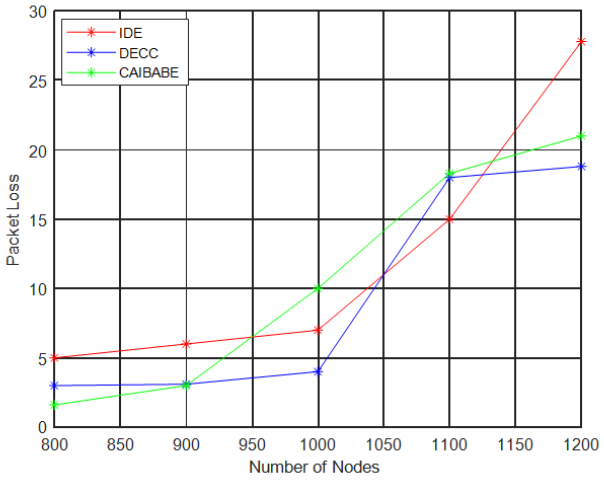

Fig 3 Output representation of Packet loss

Average Energy Consumption

The energy consumption for each node is calculated by subtracting the initial value (i) of the energy at each and every node from the remaining energy (r); the value is again divided by the total number of nodes (N).

$$\text{Average Energy Consumption} = \frac{i - r}{N}.$$

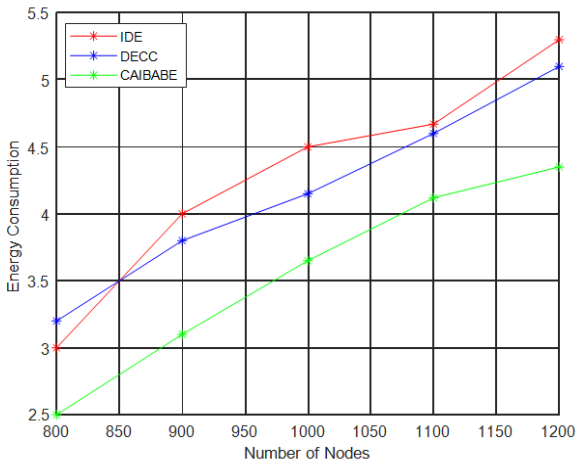

Fig 4 Energy comparison

Figure 4 shows the comparison of energy against the number of nodes for IDE, DEEC and CAIBABE.

It can be seen that CAIBABE has the lowest Routing overhead compared to IDE and DEEC, while the other IDE have the worst performance compared to DEEC

CONCLUSION

Wireless Body Area Networks supporting healthcare applications are still at an early stage of development, but already offer significant opportunities for monitoring, diagnosis and therapy. Because WBAN sensing devices are used to collect sensitive data and may encounter antagonistic situations, they require a complicated and very secure security medium or structure to avoid toxic communication within the system. These devices represent a range of security and privacy measures for sensitive and private patient medical data. When we develop a security solution for WBANs, we should make sure that it takes into account all aspects of WSNs such as privacy, integrity, data freshness, identity authentication and availability that make WBANs secure. The results of this study show that the CAIBABE method has lower energy consumption than IDE and DEEC. CAIBABE also achieves better results in other performance metrics for each speed variation.

References

[1] Zhiping Cai, Yangyang Li, Wencheng Sun, Fang Liu, Shengqun Fang and Guoyan Wang, “Security and Privacy in the Medical Internet of Things: A Review,” Journal of Security and Communication Networks, pp. 1-9 2018.

[2] Omala, A.A., Mbandu, A.S., Mutiria, K.D. et al., “Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network,” J Med Syst , vol. 42,no. 108, 2018.

[3] C. Ma and M. Li, R. Du, "Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains," inTsinghua Science and Technology, February 2023, vol. 28, no. 1, pp. 13-26,doi: 10.26599/TST.2021.9010070.

[4] K. R and K. B, "Privacy Preserving Security Integrating Method with Varying Key Encryption Model in Cloud,"2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1-9, 2022 ; doi: 10.1109/ICSES55317.2022.9914177.

[5] Y. Miao ,Y. Yang , K. -K. R. Choo and R. H. Deng, "Lightweight Privacy-Preserving Spatial Keyword Query over Encrypted Cloud Data,"2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS), pp. 392-402, 2022, doi: 10.1109/ICDCS54860.2022.00045.

[6] W. Yang, Y. Zhu ,X. Ma and Z. Bai, "A Secure and Efficient Data Deduplication Scheme with Dynamic Ownership Management in Cloud Computing,"2022 IEEE International Performance, Computing, and Communications Conference (IPCCC), pp. 194-201, 2022, doi: 10.1109/IPCCC55026.2022.9894331.

[7] Z. Li, H. Wang and H. Fang , "Group-Based Cooperation on Symmetric Key Generation for WirelessBodyAreaNetworks,"inIEEEInternetofThingsJournal,vol.4,no.6,pp,1955-1963, Dec. 2017, doi: 10.1109/JIOT.2017.2761700.

[8] A. Nabila and E. B. Mohamedand, "A QoS based comparative analysis of the IEEE standards 802.15.4 & 802.15.6 in WBAN-based healthcare monitoring systems,"2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), , 2019, pp. 1-5,doi: 10.1109/WITS.2019.8723709.

[9] H. Su, J. Liu ,X. Yuan, H. Tian, H. Wang, and A. Taherkordi, "Edge-Enabled WBANs for Efficient QoS Provisioning Healthcare Monitoring: A Two-Stage Potential Game-Based Computation Offloading Strategy," inIEEE Access, 2020,vol. 8, pp. 92718-92730, doi: 10.1109/ACCESS.2020.2992639.

[10] A.Tripathi and D. Yadav, "Load balancing and position based adaptive clustering scheme for effective data communication in WBAN healthcare monitoring systems,"2017 11th International Conference on Intelligent Systems and Control (ISCO), 2017, pp. 302-305, doi: 10.1109/ISCO.2017.7856003.

[11] J. Loane, F. McCaffery ,P. C. Paul, and G. Regan, "A Data Security And Privacy Risk Management Framework For WBAN Based Healthcare Applications*,"2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), pp. 704-710, 2021, doi: 10.1109/PerComWorkshops51409.2021.9431069.

[12] Y. Zhong ,S. Ma and Q. Huang, "Efficient Public Key Encryption with Outsourced Equality Test for Cloud-based IoT environments," in IEEE Transactions on Information Forensics and Security, 2022, doi: 10.1109/TIFS.2022.3212203.

[13] A. Catalfamo, A. Celesti, M. Fazio and M. Villari, "A Homomorphic Encryption Service to Secure Data Processing in a Cloud/Edge Continuum Context,"2022 9th International Conference on Future Internet of Things and Cloud (FiCloud), 2022, pp. 55-61, doi: 10.1109/FiCloud 57274. 2022.00015.