

# Lightweight Electronic Signatures and Reliable Access Control Included in Sensor Networks to Prevent Cyber Attacks from Modifying Patient Data

Mishall Al-Zubaidie\*

Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Thi-Qar, 64001, Iraq

**Abstract-** Digital terrorism is a major cause of securing patient/healthcare providers data and information. Sensitive topics that may have an impact on a patient's health or even national security include patient health records and information on healthcare providers. Health databases and data sets have been continually breached by many, regular assaults, as well as local and remote servers equipped with wireless sensor networks (WSNs) in diverse locations. The problem was addressed by some contemporary strategies that were created to stop these assaults and guarantee the privacy of patient data and information transferred and gathered by sensors. Nevertheless, the literature analysis outlines many indications of weakness that persist in these methods. This study suggests a novel, reliable method that bolsters the information security and data gathered by sensors and kept on base station datasets. The proposed approach combines a number of security mechanisms, including symmetric cryptography for encryption, asymmetric cryptography for access control and signatures, and the Lesamnta-LW method in the signature process. Users' information is shielded from prying eyes by the careful application of these measures and a sound approach. Investigational comparisons, security studies, and thorough results show that the suggested method is better than earlier methods.

**Keywords:** AES-192, ACM, data tampering, NGAC, Lesamnta-LW, SAML, sensor networks, vampire

## 1 Introduction

Electronic applications by the Internet of Things (IoT) have provided many benefits to users and multiple organizations; One of its most important features was the expansion of services, communications, dealing with big data, and providing all kinds of information (audio, video, image, text ... etc.) for the different healthcare systems. Consequently, these systems are increasingly required to support patient-doctor communication activities that take place in that environment and directly [1]. It is the use of patient data in digital form that increases the likelihood that some users or suspicious organizations will engage in malicious activities online that may lead to psychological, physical, moral and/or economic harm. These malicious activities became known by the term "data terrorism" or "digital terrorism". In a healthcare application scenario, these threats can be in a variety of ways, such as destroying a computer system in a health center or exposing patients' private medical data in a health database to the public. Whatever methods the attacker uses, the general and specific effects are the same: sensitive patient data and patient care are seriously compromised, the acceptability of the health care system fails, and services are not guaranteed. In addition, there is evidence indicating that cyber threats are increasing and that a large part of health care systems are not equipped to counter these threats (digital terrorism), for example, Figure 1 illustrates how digital terrorism affects electronic applications across many industries, whereas the healthcare industry is subject to a higher percentage (23%) of cyberattacks than other industries. Securing

---

\*Corresponding author: e-mail: mishall\_zubaidie@utq.edu.iq).

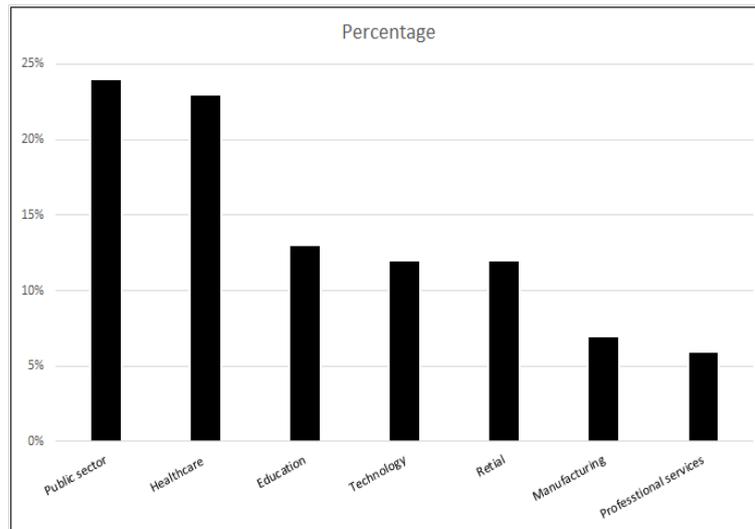


Figure 1: Cyberthreats and data breaches in several crucial industries [8]

the patient data carrier is not easy because threats are constantly evolving and in a variety of ways, and with the realization that cyber terrorism must be part of a broader strategy to regulate and manage the risks of digital data, there are many mechanisms and techniques that healthcare organizations can use to protect digital health data of electronic threats [2].

The preserve privacy of medical data in the health systems such as electronic health records (EHRs) has been a major importance to academic, research and health organization, since the quality and efficiency of medical records management [3] by utilizing the Internet. For authorization privileges to control access to information and patients' data within EHR systems, authorization privileges are required [4]. Accurate health information is essential for diagnosing illnesses and characterizing medical conditions when patients' medical data are transferred electronically from patient to provider [5]. Patients suffer severe complications from any alternative to these records. Additionally, patients may experience harassment, discrimination, or even pass away if the diagnostic findings for illnesses like dermatological or HIV infection alter while being sent from sender to recipient [6]. Terrorist actions have the potential to increase national vulnerability and insecurity through the disclosure of user records, the alteration of records, the erasure of records, or the impersonation of users inside health systems. EHR approaches should present edge-to-edge security for users' records. A central server can also enhance data management but is a tempting target for hackers because it stores medical records and authorizes users (patients and providers) by privacy policies [7]. To prevent a breach of the server's policy and protect the privacy of patient records, privacy mechanisms are essential. A major challenge for authorization schemes is how to utilize patients' records for a variety of purposes like access by family members, consultations, caregivers, emergency situations and medical research (indirect/secondary utilization). For instance, the doctor researcher must not override the permissions of privacy allowed to him/her. A patient's privacy is vigorously compromised, in case of emergency, when the physician is unavailable or the patient cannot consent to another provider [9]. Moreover, the patient's records must be received by a relative if the patient is incapacitated [10]. When operating on a patient, it is sometimes necessary for the doctor to consult with another physician. Medical records could be penetrated and accessed by all of these circumstances. When medical records are exchanged between patients and EHR providers, malicious threats have the potential to misuse or abuse them [11]. Numerous incidents of breaches into databases and medical records of patients have occurred, including

- Attackers posing as patients gained access to SingHealth’s clinic and clinic datasets on July 20, 2018, the largest health operator in Singapore. The attackers next illegitimately accessed and penetrated medical records on 4 July 2018. The medical records of 1.5 million Singaporeans inclusive of records belonging to Prime Minister Lee Hsien Loong were penetrated [12].
- In May 2021, a ransomware attack breached the California hospital platform, causing their patient portal to go offline and EHR activities to be interrupted [13].
- Effective attacks to healthcare applications include the May 2021 Scripps Health cyberattack and the January 2022 Kronos incident [14].

The security lapses clarify why robustness and excellent security are necessary for health applications. Because every patient and provider has privileged access to a server dataset, an inside danger can likewise access a medical record more readily than an external one. The suggested protocol included next-generation access control (NGAC) to offer strong security based on roles and provider/patient characteristics. Therefore, while guaranteeing the security of medical information, health sensor systems schemes must include procedures that preserve healthcare user/sensor information, authorization policies, and patient privacy demands [15].

## 1.1 Threat to Authorization Approach

An analysis of the drawbacks of many health applications requires the construction of a threat model. The threat model [16] and [17] that named Dolev-Yao is utilized to check users’ authorization in proposed approach. It is a practical/formal manner of analyzing authorization protocols in actual applications. This model is efficient in testing and analyzing different threats. This proposed supposes that threats could be passive, active, external and internal. Furthermore, it assumes that the attributes server (AS) is reliable and secure in resistance to information databases breakthrough threats. Thus, this model addresses the following attacks:

- Information logging at a particularly crucial location may be interrupted if the health wireless sensor is prevented from sending data or connecting to the network (node outage).
- Gaining unauthorized access to the health network by using a Man-in-the-Middle threat to change patient records.
- Utilizing an impersonation threat to obtain medical records in order to send a counterfeit authorization message.
- Increasing the pace of a rogue node during the routing process in order to obtain health sensor packets before the time is due (rushing attack).
- Consuming the power of sensor nodes and stopping the network altogether (vampire attack).
- Sending raw data to the wrong node and selecting the longest path to traverse (neglect and greed attack).
- The captured data packet might be dropped by a rogue node, which is always ready to reply to the route request (packet drop attack).

## 1.2 Objectives of Study

The authorization approach aims to achieve the following tasks:

- Combining features and roles models: The suggested method integrates two authorization models (RBAC and ABAC) in the NGAC model to facilitate the management of patient data at the roles and attributes levels;
- Adding digital signatures to security assertion markup language (SAML) requests: SAML representations must have integrity and anonymity for the subjects’ wishes and regulations;

- Utilizing a digital signature mechanism and secrecy sharing scheme: The suggested method for granting users and sensors permission is predicated on the exchange of Shamir secrets with digital signatures (ECDSA);
- Combining Lesamnta-LW and ECDSA: This goal makes it possible to employ lightweight ECDSA-Lesamnta-LW signatures rather than ECDSA-SHA-1, particularly when sending data gathered by WSN;
- Hiding information and data stored in network requests: The proposal accomplishes encryption and decryption operations by applying AES-192 cryptography with 10 rounds to prevent attackers from gaining access to the security parameters of users and the network.

The remainder of the research is structured as follows. In Section 2, we describe the design of QDFaultInjector, our framework for fault injection testing of kernel modules, in detail. In Section 3, we design some corresponding experiments to evaluate QDFaultInjector. In addition, QDFaultInjector is compared with several existing fault injection tools and a brief summary is made in Section 4.

## 2 Overview of Current Authorization Approaches

This section highlights the shortcomings of authorization policies intended to safeguard healthcare users inside a health network, based on relevant existing standards.

Seol et al. [18] introduced combining the ABAC model with both XML and XACML to support electronic signatures and encryption in the EHR [19]. Their model uses partial encryption with signature XML files to provide security for cloud environments with EHR. Their model implements two phases of using XACML to provide authorization requests and using XML with signature and encryption to provide data protection [20]. Nonetheless, there are several privacy issues associated with a cloud environment with EHR because it is possible to use the same data from multiple organizations or health institutions which can cause privacy issues. Furthermore, the use of public key cryptography with XML requests and responses can incur a significant cost to model performance. Also, some authorization requests and responses are sent explicitly, causing some authorization parameters to be exposed by attackers.

Zaghloul et al. [21] proposed a decentralized scheme for sharing health data based on privacy and security features. Their scheme leverages blockchain technology and smart contracts to support privacy. They indicated that their scheme allows for the disclosure of certain pieces of data based on patient selections and privacy preferences. However, their scheme does not provide sufficient security analysis to document the protection of patients' health records. Also, the disclosure of certain parts of health data by patients is a clear breach of privacy, as not all patients have an adequate security culture. Designing a scheme based on patients' choices/selects will not be convincing for patients on the one hand and health institutions on the other.

Saini et al. [22] established an architecture to secure health record sharing in an electronic medical record (EMR) and eliminate a single-point problem of failure. Smart contracts, access control, activity detection, and revocation were the four states that their framework employed. They stated that massive data for health databases was managed by their framework. The Edwards-curve digital signature algorithm (EdDSA) is used to achieve the signature, and its framework makes use of elliptic curve cryptography (ECC). The authors did not, however, specify how well their system would defend against attacks. Additionally, using ECC encryption in healthcare institutions when working with large amounts of data might be expensive.

To enhance data management and privacy in EMR records, Chen et al. [23] combined public and private clouds. They created the public-key algorithm-based EMR authorization system, which safeguards patient medical records. They asserted that their system enables integrity, backward and forward security, non-repudiation, unlinkability, anonymity, and protection against replay, man-in-the-middle, and impersonation. However, their approach lacks the anti-traceability and anti-leakage capabilities that are critical to any trustworthy authorization system that offers strong data privacy, as well as tools to prevent DoS and dataset assaults.

Wu et al. [24] created a way to authorize users in the EHR health system using a blockchain and patient privacy-preserving approach to access control. They point out that strong safeguards are necessary to stop data leaks in the health information system involving private medical information. To secure authorization requests, their approach uses file authorization contracts and common cryptographic techniques. Nevertheless, information regarding authorization requests and policies regarding their acceptance or rejection is not provided by this means. Additionally, file authorization contracts for source-restricted devices like WSN do not depend on a thin performance support mechanism.

Similar to [22], Shuaib et al. [25] suggested a decentralized file healthcare system for EHR that applies a threshold signature to eliminate the problems of DoS attacks and a single point of failure. They proposed a consensus manner for the design of Istanbul Byzantine fault tolerant (IBFT). Although a decentralized system design is beneficial in reducing a single point of failure, their system can cause copies of unwanted and redundant authorization requests and the system will require larger resources to implement. Also, the authors address the danger of DoS but do not address the dangers of impersonation and internal attackers accurately.

According to Fareed and Yassin [26], they suggested a privacy plan for health systems that supports scalability, dynamism, and security risk tolerance by utilizing the RBAC approach and multi-factor authentication. Their plan employed symmetric encryption and hash methods to authenticate users and an asymmetric encryption system that relied on Schnorr's signature to offer multi-factor authentication for the administrator. Their plan, however, clearly violated security as it only protected the administrator's requests and not those of other users. Furthermore, their schema only used user roles to safeguard permission requests, which was insufficient to support privacy because it only used the RBAC approach.

Lastly, Zala et al. [5] suggested creating a patient record management strategy to satisfy e-health standards. They looked into applicability and throughput concerns. The authors also demonstrated the applicability of their approach by comparing its security to that of the Robust Healthcare-Based Blockchain (SRHB). They noted that privacy is crucial in e-health and cloud computing environments, and that the majority of health applications conceal health data using AES-128 encryption. However, the authors neglected to mention that internal attacks pose a greater risk to health authorization systems than external ones. Additionally, their plan lacked a safeguard against alteration and a mechanism for data integrity.

### 3 Introductory Conceptions of Authorization Mechanisms

To provide a reliable authorization scheme, it requires studying privacy mechanisms and clarifying some details in building user authorization rules and policies in EHR health applications. Therefore, privacy concepts require the adoption of robust mechanisms to support the privacy preservation of data collected from WSN and the security of data stored in servers. The data collected by WSN is transmitted in an insecure medium by IoT in EHR systems which also requires privacy mechanisms for preserving patient data. In this section, a set of basic mechanisms are briefly explained:

- Symmetric encryption mechanism

There are many symmetric encryption algorithms that rely on a shared key in protecting records in health databases, the most prominent of which is the advanced encryption standard (AES) or Rijndael, introduced in 2001 by the National Institute of Standards and Technology (NIST) [27]. AES encryption is an upgraded version of the data encryption standard (DES) and Triple DES, proposed in January 1999. AES was designed to eliminate the security problems that DES had with compromised attacks where DES uses a 56-bit key. The AES algorithm is a 128-bit block cipher, also, this algorithm has different key lengths to block attacks such as 128, 192, and 256. Figure 2 shows the encryption and decryption processes in the AES algorithm. Each block cipher is split into 16 bytes in a 4\*4 state array. This algorithm consists of 10, 12 and 14 rounds. To mix the data with the symmetric encryption key, each round includes Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key processes [28, 29].

Substitute Bytes process is nonlinear transformation and invertible, during this process, the 8-bit (byte) of the state array is commuted with a byte in the substitution box (S-box). This process uses a

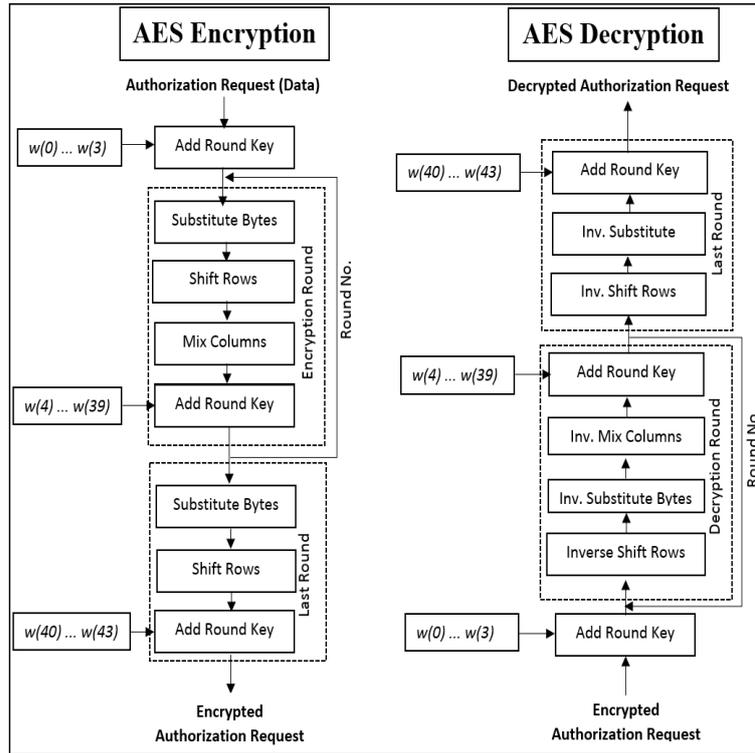


Figure 2: AES algorithm for encryption and decryption

lookup table that contains 28 words divided into bytes. This step is useful to prevent the connection between the encrypted data and the encryption key from being exposed. Using 8-bit input data, S-box locations are addressed based on the most significant and least significant nibbles. In the Shift Rows process, a predefined offset is applied to each byte in the state array rows [30]. There is no change to each of the bytes in the first row, but each of the bytes in the second row is shifted one position to the left of the original. Similarly, the third and fourth rows are shifted two and three positions to the left, respectively. Mix Columns processing is performed in all rounds except the last round. The MixColumns process, it multiplies each column by a modular polynomial in  $GF(2^8)$ , instead of calculating separately. Alternatively, the SubBytes and MixColumns processes can be joint into large Look-Up Tables (LUTs). The MixColumns process mixes the columns of the state array linearly. The Add Round Key process applies the derived round key to the data block to secure the data. After the main key has been expanded, a subkey is derived, resulting in a key array of 176 bytes in 44 words (using a key length of 128 bits). Each byte of the block was XORed with the corresponding byte in the round-key. The decryption process in AES is performed opposite to the encryption process. Decryption takes ten rounds in AES for keys with 128 bits, twelve rounds for keys with 192 bits, and fourteen rounds for keys with 256 bits. However, the round of the decryption procedure divided into Inverse Sub Bytes, Inverse Shift Rows, Inverse Mix Columns and Add Round Key (Figure 2 shows decryption process).

- Data integration mechanism

Integration of health records is a very important issue to ensure that patient data and reports remain unchanged [31]. ECDSA, or elliptic curve digital signature algorithm, is an asymmetric signature mechanism introduced by Scott Vanstone in 1992 [32]. This algorithm is designed to supply au-

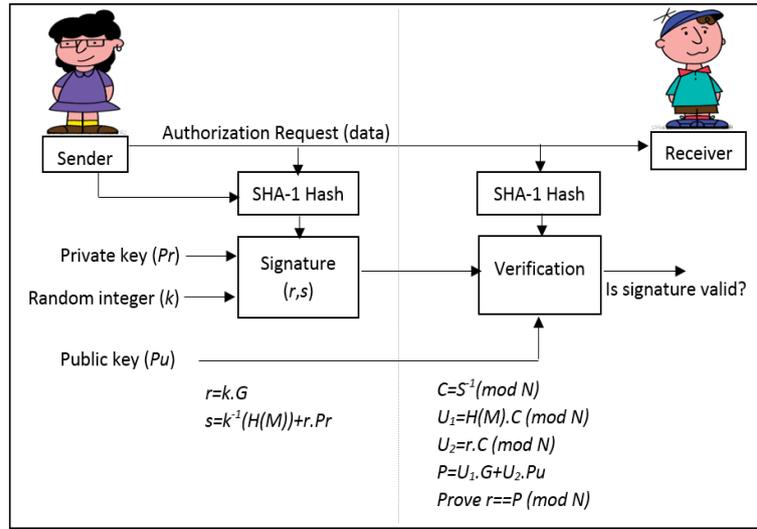


Figure 3: ECDSA algorithm for signature and verification

Authentication, integrity and non-repudiation requirements. In conventional digital signature algorithms (DSA), primes  $p$  and  $q$  are selected and  $q|(p-1)$  and  $G$  are subgroups of order  $q$  of  $Z * p$ . Multiplication modulo  $p$  is then performed on  $G$ . Function  $H'$  is defined by  $H'(R) = R \text{ mod } q$  [33]. It contains a cyclic group of prime order  $q$ , a generator ( $g$ ) for  $G$ , and two hash functions  $H : [0, 1] \rightarrow Zq$  and  $H' : G \rightarrow Zq$ . ECDSA is a development of the DSA algorithm based on elliptic curves. As long as the parameters of this algorithm are carefully chosen, the ECDLP enables it to block various attacks when using points on the curve for signing data and information. This algorithm generates the private key ( $Pr$ ) and a random number ( $k$ ) to calculate the public key ( $Pu$ ) through  $Pu = Pr.k$ . Therefore, ECDLP means that it is very difficult for an attacker to extract  $k$  from  $Pr$  and  $Pu$ . This algorithm relies on small parameters which it produces smaller keys compared to other asymmetric algorithms like RSA. This case makes this algorithm very suitable for handling big data in health institutions as well as being applicable to source-restricted devices such as WSN and RFID. Sensors and network devices require the use of a robust and high-performance mechanism to ensure data integrity because complex computations in some public key algorithms cause loss of sensor resources such as power and storage [34, 35]. Specifically, source-restricted devices need appropriate routing protocols [36] and security protocols with a high level of security. Figure 3 shows signature and verification processes in ECDSA [33]. However, the ECDSA algorithm relies mainly on SHA-1 for its operations, since SHA-1 produces a message digest of length 160 which is not very safe against attacks. In addition, SHA-1 does not offer high performance compared to lightweight hash algorithms. Therefore, one of the weaknesses of the ECDSA algorithm is SHA-1 [37].

- One way hash function mechanism

Hash functions of all kinds, whether standard or lightweight, produce a fixed-length MD [38]. It is very useful for producing a hex value that cannot be decoded or used to extract the original text. The hash is evaluated based on its resistance to collisions, preimage and second preimage. Standard hash functions include MD5 and SHA-1, while lightweight hash functions include Lesamnta-LW (LLW), ARMADILLO, GLUON, LHash, and DM-PRESENT. This proposal focuses its study on the LLW algorithm because it has advantages in supporting resources, especially in resource-constrained devices. Among the methods recommended by NIST, the lightweight cryptography initiatives include LLW, PHOTON, and SPONGENT for hashing. On an 8-bit processor, LLW needs only 50 bytes of RAM (similar to AES' S-box structure), and is five times faster than SHA-256 [39, 40]. A new family

Table 1: Performance comparison between Lesamnta-LW and other hashing algorithms

Name	Techno. ( $\mu\text{m}$ )	No. of GEs	Throughput (Kbps @ 100kHz)
ARMADILLO	0.18	(2923/4353/5406/6554/8653) vs. (4030/6025/7492/8999/11,914)	(27/250/250/25/25) vs. (109/1000/100/100/100)
DM-PRESENT	0.18	(1600/1886) vs. (2213/2530)	(14.62/22.9) vs. (242.42/387.88)
H-PRESENT	0.18	2330 vs. 4253	11.45 vs. 200
GLUON	–	2071/2799.3/4724	12.12/32/58.18
Lesamnta-LW	0.09	8240	–
LHash	0.18	817/817/1028	2.40/2.40/(1.81, 0.91)
PHOTON	0.18	(865/1122/1396/1736/2177) vs. (1168/1708/2117/2786/4362)	(2.82/1.61/2.7/1.86/3.21) vs. (15.15/10.26/20/15.69/ 20.51)
QUARK	0.18	(1379/1702/ 2296) vs. (2392/2819/4640)	(1.47/2.27/3.13) vs. (11.76/18.18/50)
sLISCP	0.065	2271/3019/3019	29.62/44.44/22.22
SPN-Hash	0.18	(2777 / 4625) vs. (4600 / 8500)	(36.1 / 35.8) vs. (55.7 / 111.3)
SPONGENT	0.13	(738 / 1060 / 1329 / 1728 / 1950) vs. (1127 / 1687 / 2190 / 2903 / 3281)	(0.81 / 0.34 / 0.4 / 0.22 / 0.17) vs. (17.78 / 11.43 / 17.78 / 13.33 / 11.43)

of cryptographic hash functions has been submitted to NIST as part of a competition to develop cryptographic hash algorithms.

LLW uses many versions of MD such as 224, 256, 384 and 512. An LLW is a plain Merkle-Damgard iterated hash algorithm, taking as input a key that is  $n/2$  bits and a plaintext that is  $n$  bits, where  $n$  is an even number. LLW, for instance, uses AES as its underlying cryptographic primitive, while SHA-256 uses SHACAL-2. Sensors and RFID devices that use restricted resources require security hash functions [41, 42, 43]. LLW uses 256-bit plaintext and 128-bit keys with an AES-based block cipher. LLW only contains the length of data input in last block, not any parts of data, in Padding. The preimage resistance of LLW is ensured by this feature. In this function, 64-round block ciphers are used. The key is 128 bits long and the input data is 256 bits long. A one-key scheduling algorithm is used in the first phase of LLW’s block cipher, and a one-key mixing algorithm is used in the second phase to generate ciphertext by using data and round key. In the mix function, XOR operations, word-wise permutations, and a non-linear function  $Gf.PQ = MixColumns.SubBytes$  are combined. Where  $SubByte$  is a non-linear substitution operation. The input is divided into four bytes ( $s_0, s_1, s_2$  and  $s_3$ ) and then the substitution box ( $S_i' = S - Box(S_i)$ ) is implemented. The  $MixColumns$  operation is defined by the AES maximum distance separable matrix multiplication given by  $GFe(2^8)$  [41]. More details about this algorithm are available at [44]. The following Tables 1 and 2 show a comparison of performance and security features between Lesamnta-LW and other hash functions[45].

- Authorization control models

A medical records access control model is a mechanism that checks users’ privileges against authorization policies to preserve the confidentiality of medical records [46]. These privileges are specified by a database system (DBS) authorization administrator or privacy officer. These authorizations could be specified by following either a DAC policy, MAC policy, RBAC policy, or ABAC. Each authorization system requires access control model (ACMs) to authorize users’ access to the medical records. Many ACMs, and each model relies on a specified manner and set of rules. Table 3 shows the differences between the control models (DAC, MAC, RBAC and ABAC). However, the ACMs most used in recent research and applied in health applications are RBAC and ABAC.

Table 2: Comparison of security features between Lesamnta-LW and other hashing algorithms

Name	Construction	Type of compression function	Message digest (bits)	IS (bits)	Rate (bits)	Preimage	Second preimage	Collisions	Best known attack
ARMADILLO2	MD	BC with data-depend. bit transpositions	80/128 /160/192/256	256/384 /480/576/768	48/64 /80/96/128	$2^{80}/2^{128}$ / $2^{160}/2^{192}$ / $2^{256}$	$2^{80}/2^{128}$ / $2^{160}/2^{192}$ / $2^{256}$	$2^{40}/2^{64}$ / $2^{80}/2^{96}$ / $2^{128}$	Practical free-start collision attack $2^{8.9}/2^{10.2}/2^{10.2}/2^{10.2}/2^{10.2}$
DM-PRESENT	MD	PRESENT in Davies-Meyer mode	64	64	80 / 128	$2^{64}$	$2^{64}$	$2^{32}$	Multi-differential collision attack $2^{29.18}$ hash comp. on 12 rounds
H-PRESENT	MD	PRESENT in double-block-length c.	128	128	64	$2^{128}$	$2^{128}$	$2^{64}$	–
GLUON	T-sponge	Based on Feedback with Carry Shift Register	128/160/224	136/176/256	8/16/32	$2^{128}/2^{160}$ / $2^{224}$	$2^{64}/2^{80}$ / $2^{112}$	$2^{64}/2^{80}$ / $2^{112}$	Preimage attack $2^{105}$ complexity
Lesamnta-LW	MD	Type-1 GFN 64-round BC in LW1 mode	256	256	128	$2^{120}$	$2^{120}$	$2^{120}$	–
LHash	P-Sponge	18-round Feistel-PG	80/96	96/96	16/16	$2^{64}/2^{80}$	$2^{40}/2^{40}$	$2^{40}/2^{40}$	–
PHOTON	P-Sponge	12 round AES-like permutation	80/128/160/224/256	100/144/196/256/288	(20,16)/16/36/32/32	$2^{64}/2^{112}$ / $2^{124}/2^{192}$ / $2^{224}$	$2^{40}/2^{64}$ / $2^{80}/2^{112}$ / $2^{128}$	$2^{40}/2^{64}$ / $2^{80}/2^{112}$ / $2^{128}$	–
sLISCP	P-Sponge	Type 2 GFN Simeck	160/160/192	192/256/256	32/64/64	$2^{128}/2^{128}$ / $2^{160}$	$2^{80}/2^{96}$ / $2^{96}$	$2^{80}/2^{96}$ / $2^{96}$	–
SPN-Hash	P-Sponge	SPN permutation in JH mode 10 rounds	128/256	256/512	128/256	$2^{128}/2^{256}$	$2^{128}/2^{256}$	$2^{64}/2^{128}$	–
SPONGENT	P-Sponge	PRESENT-like permutation 45/70/90 /120/140 r.	80/128/160 /224/256	88/136/176 /240/272	8/8/16/16 /16	$2^{80}/2^{120}$ / $2^{144}/2^{208}$ / $2^{240}$	$2^{40}/2^{64}$ / $2^{80}/2^{112}$ / $2^{128}$	$2^{40}/2^{64}$ / $2^{80}/2^{112}$ / $2^{128}$	Linear distinguishers on 23 rounds of the SPONGENT permutation

The RBAC model is used as an option substitute for the DAC and MAC models. This concept was developed by David Ferraiolo and Rick Kuhn in 1992, in which the system administrator creates roles and grants rights to those roles according to the functions performed in an organization. Data access privileges and rights are associated with each role in RBAC's system, which makes it secure as a result of its structure of assigned roles to users. This ACM categorizes users by roles such as patient, doctor, advisor, researcher ... etc., each with its own privileges and rights. Roles in the system are assigned to clients depending on their jobs. Since roles function as a connect between data access modes and clients, RBAC is better suited and less complexity for health environments than DAC and MAC [47].

ABAC is one of the promising alternatives, which evaluates conditions, data attributes, and user attributes, as well as policies specifying those conditions and attributes. The ABAC model has recently drawn significant interest for protecting the privacy of medical records. This ACM utilize client attributes (like name, job, address, sex, age, marital status, phone number, location, time and health status) to authorize clients to access the server's health database more accurately (fine-grained) and privately [32]. The ABAC model proposed in 2011 to overcome the limits in the most widely famous control access models (DAC, MAC, and RBAC). Due to the wide range of attributes it addresses, ABAC is a rich model. Cloud computing, IoT, Big Data, VANETs, Internet of Things and especially healthcare all have applications where ABAC supports administration, authorization, risk intelligence, and scalability. ABAC categorizes attributes into subject, object, action, and environment. After extensive review of the ACM models, it is clear that the RBAC and ABAC models have important advantages in supporting the privacy of medical records and are well suited to this proposal [48].

Table 3: Differences between control and access models

Factors	DAC	MAC	RBAC	ABAC
Access Control to Information	Through owner of data	Through fixed rules	Through roles	Through attributes
Access Control Based on	Discretion of owner of data	Classification of users and data	Classification of roles	Evaluation of attributes
Flexibility for Accessing Information	High	Low	High	Very high
Access Revocation Complexity	Very complex	Very easy	Very easy	Very easy
Support for Multilevel Database System	No	Yes	Yes	Yes
Used in	Initial Unix system	The U.S. department of defense	ATLAS experiment in CERN	The Federal government

- Data management and control mechanism

In the proposed approach, the EHR database is an exceedingly important component. TAs health systems struggle to deal with a wide range of coordination for medical records, the repositories store data and information in different forms. Extensible access control (XML) is therefore suitable for online data transfer of many kinds. XML, being a symbolic language, employs an easy and adaptable process to describe, exchange, and handle data in online settings [49].

Nevertheless, XML files should support various levels of data security for sensitive data throughout the file or in parts of it [50]. Access to medical records is a considerable issue in big data management systems that utilize various mechanisms. Furthermore, the interchange of data online has become essential and requires to perform access authorization, especially in EHR approaches. Access control and XML-based data management are both covered by the extended access control markup language (XACML) standard. At a fine-grained level, XACML offers flexible and efficient data access and authorization properties [51]. It contains numerous qualities that make it appropriate for online use, and it is supplied by the organization for the improvement of structured information standards (OASIS). Policy, algorithm, attribute, numerous subjects, policy distribution, implementation independence, and duties are a few examples [51].

Prior to using units like policy enforcement points (PEP), policy decision points (PDP), policy administration points (PAP), policy information points (PIP), and policy retrieval points (PRP), XACML uses certain policies to assess access requests. XACML operations are depicted in Figure 4 [49] (PEP transmits and receives requests and access responses to the database; PDP evaluates decisions; PAP creates policies based on user attributes; PIP recovers user attributes; and PRP retrieves user data from the database). Through PEP, the subject receives the decision outcome (permit, refuse, not applicable, or indeterminate).

- Secret sharing mechanism

Secret-sharing mechanisms are typical secure multi-party calculation protocols [52]. With prime fields, it is locally leakage-resistant to arbitrary one-bit leaks from each secret share. A master secret ( $MS$ ) is generated by a set of secret sharing ( $SS_s$ ) and threshold ( $t$ ) in the Shamir or secret sharing scheme ( $SS_s, t$ ). Some or all of the  $SS_s$  could be used to generate the master secret. This mechanism specifies the minimum number of secrets required to reconfigure  $MS$ . This mechanism includes the generation and reconstruction phases [53]. Clients ( $C_i$ ) receive one secret sharing ( $SS$ ) from the server as part of the generation phase ( $MS$ ) is split into a set of secrets sharing ( $SS_1, SS_2$ , etc.). Reconstruction requires  $C_i$  to perform any set of secrets ( $SS_s$ ), depending on  $t$ , to reconstruct  $MS$ , this ensures homomorphism and correctness features. This guarantees the secrecy feature since  $C_i$  cannot obtain information from the server while  $t-1$  from  $SS_s$ . Hackers have a hard time figuring out the  $MS$ , and the secrets set up for the  $MS$  are anonymous [54]; they have no way of knowing if they belong to particular individuals. The Shamir mechanism provides an anonymous method for creating a  $MS$

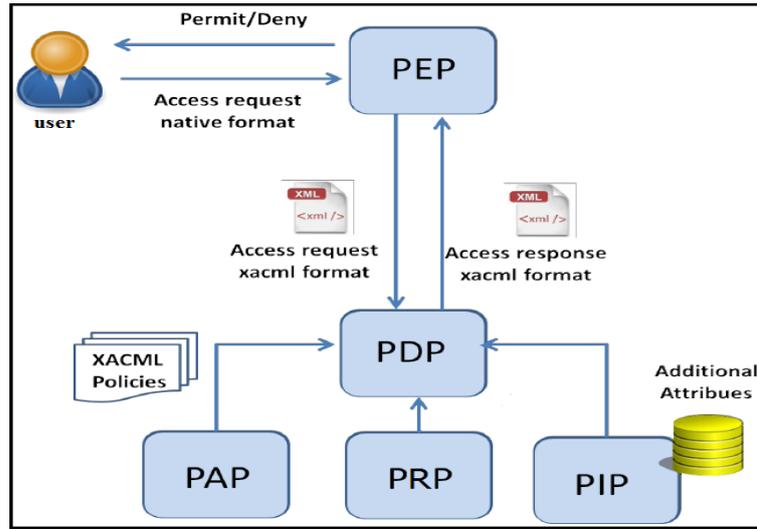


Figure 4: XACML architecture

with a number of features, including ease of creating a  $MS$  from a group of secrets, development of a new secret for one-time use, a  $MS$  size equal to  $C_i$ 's  $SS_s$  sizes, and complete security in hiding  $C_i$ 's  $SS_s$ . Figure 5 [55] describes the use of the Shamir scheme to create the secret from the users' secret set. Nonetheless, Shamir mechanism is still to be vulnerable to penetration.

- The wireless communication environment is considered an insecure medium for unprotected transmission of network members' secrets, which could put patient data at risk.
- Collecting  $t$  shares to retrieve the master secret key is a complex problem in the connections of large networks with a huge number of members.
- Assuming all network members are honest and loyal in a large network of hundreds of patients and providers is a naive strategy.
- Distributing each member's role in helping others rebuild and recover the master secret may overburden the server due to the high communication between network members.
- Any authorized member with access to network services and broadcast shares can reassemble the polynomial and discover the secret key. Therefore, any legitimate malicious member can supply a forged secret without anyone finding out.

## 4 The Recommended Approach for Authorizing Credible Sensors and Users

This section presents the technique for the suggested authorization approach that provides privacy-preserving methods to guarantee member sensors'/users' authorization in medical care apps. The symbols used in this study are described in Table 4.

### 4.1 Model of the Network

Anonymity with the SAML is an authorization method that functions with health sensor networks, as shown in Figure 6. The user ( $U_i$ ), sensor ( $Sen_i$ ), cluster head ( $Cl_i$ ), basestation server ( $BS$ ), information server ( $IS$ ), and repository server ( $RS$ ) are the elements that make up the network model. These entities

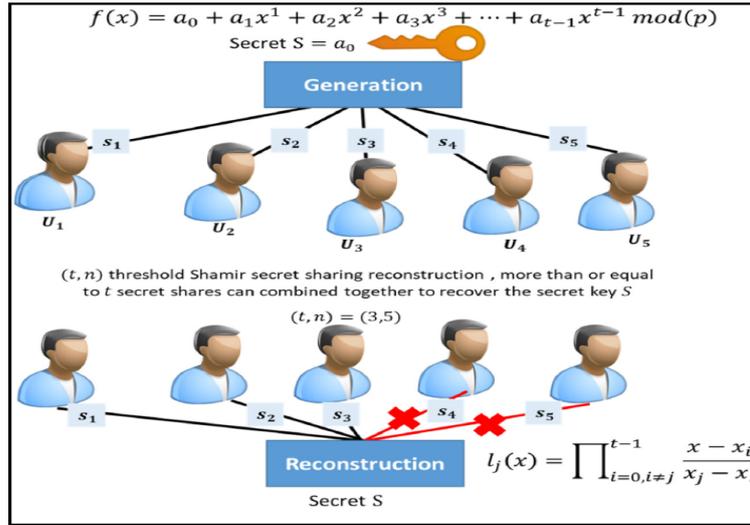


Figure 5: Shamir threshold scheme

Table 4: Manuscript's symbols

Notations	Description
$U_i, Sen_i; BS, IS$ and $RS$	User entity, Basestation, Information and Repository servers
$Sen_S, BS_S, IS_S$ and $RS_S$	Signatures generated by $Sen, BS, IS$ and $RS$
$E_{AES}, D_{AES}$	AES Encryption and Decryption
$EC_{SHA}, EC_{LLW}$	ECDSA with SHA-1, ECDSA with Lesamnta-LW
$SS$	Shamir secret
$Sen_N, BS_N, IS_N$ and $RS_N$	Random nonces and random secret nonce
$TS_i$	Time stamp
$V_{tm}$	Temporary value
$Sen_{ID}, BS_{ID}, IS_{ID}$ and $RS_{ID}$	$Sen, BS, IS$ and $RS$ identifiers
$\parallel, \oplus$	Concatenation operation, Exclusive or operation

interact with one another in the suggested approach to ensure authorization and safeguard the privacy of users and sensors when they access the health repository. Users and sensors are unable to connect directly to  $IS$  and  $RS$  due to the  $BS$  gateway. The  $Sen_i$ /providers information on the information server ( $IS$ ) is kept apart from the patient dataset on  $RS$ . Each  $U_i/Sen_i$  generates an access request, which is then transmitted to the  $BS$ . Once the authorization details for  $U_i$  or  $Sen_i$  have been verified,  $BS$  forwards the authorization request to  $IS$  for validation; in the event that the request is deemed invalid,  $BS$  replies "reject" to  $U_i/Sen_i$ .  $IS$  analyzes the permission request it receives from  $BS$  after validating the access request and confirming signatures and other security parameters. If all tests and assessments are valid,  $IS$  requests that  $RS$  retrieve/store patient data; if not,  $IS$  replies to  $BS$  with a "reject" message. This means that  $RS$  looks for security parameters (SP) and signatures (Sigs). If everything has been done correctly,  $RS$  then transmits the required information to  $IS$ , which in turn sends the "accept" answer to  $U_i/Sen_i$  by  $BS$  to permit access to and storage of the medical records. The approved  $U_i/Sen_i$  will receive the "accept" answer and a copy of the required data. To provide a high degree of  $U_i/Sen_i$  privacy, this method concentrates on protecting/storing data and requests. The open-source project that uses SAML v2.0 is responsible for protecting patient data confidentiality.

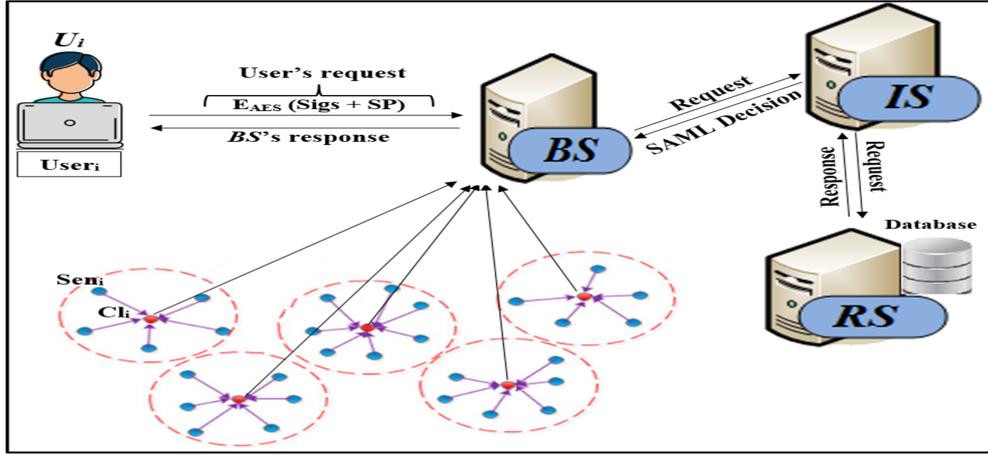


Figure 6: Proposed authorization approach

## 4.2 Developing the Suggested Authorization Strategy

In this section, we shall outline the privacy implications of the suggested permission strategy.

- **Combining the signatures of ECDSA, and Lesamnta-LW**

To ensure that security standards are satisfied with respect to the integrity of patient data, the suggested authorization mechanism uses ECDSA-256 in conjunction with policies and requests. We have implemented ECDSA signatures with senders' and receivers' information to ensure the integrity property, which prevents changing information in policies and requests; the authentication property, which prevents external hackers; and the non-repudiation property, which prevents authorized sensors/users from denying their requests to receive medical data. Implementing security criteria is essential in systems that handle sensitive data, such health sensor systems. While the  $U_i/Sen_i$  sign the request using parameters ( $Sen_N$  and  $BS_N$ ), the servers ( $BS$  and  $IS$ ) check the request's Sigs. The  $IS$  forwards the request to the SAML v2.0 evaluation procedure if it is valid; if not, it is rejected. The suggested authorization method uses ECDSA's Sigs to partially hide the  $Sen_i$  and  $BS_i$  information when sending and receiving SAML requests. This algorithm's appropriate performance and security level make it acceptable for usage in large systems that leverage health sensor technologies. We employed Lesamnta-LW in ECDSA rather than SHA1 to assist the security and performance of our approach, which has a good impact on health sensors. Lesamnta-LW is utilized in ECDSA because it supports ECDSA signatures to increase security and offers superior performance when working with sensors.

- **Administration of policies in the suggested Approach**

By using SAML, the system administrator is in charge of constructing policies for patients and healthcare providers in  $IS$ . SAML policies define the rules and conditions for how SAML assertions should be handled and enforced within an authentication and authorization system. SAML policies:

- Authentication policies: These policies specify the requirements for authenticating sensors/users before granting access to a service. They can include factors such as username/password authentication, multi-factor authentication (MFA), or integration with external identity providers for federated authentication.
- Attribute release policies: These policies determine which attributes of a user's/sensor's identity should be included in the SAML assertion sent from the IdP to the SP. Attribute release policies often involve mapping and transformation of user attributes between different identity systems.
- Authorization policies: These policies define the rules for granting or denying access to specific resources or services based on the information contained in the SAML assertion. They can be

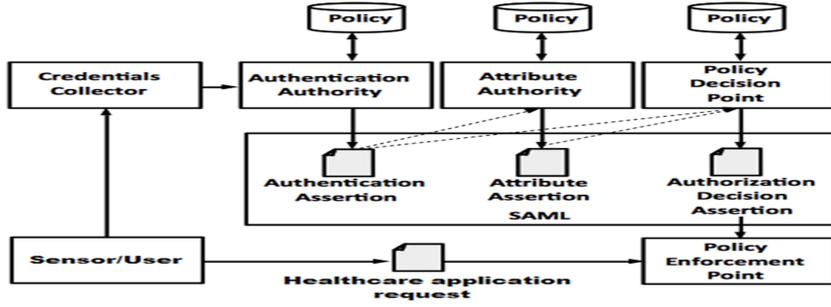


Figure 7: Proposed authorization approach policy

based on attributes such as user/sensor roles in the NGAC model, group memberships, or custom attributes defined in the SAML assertion.

Figure 7 displays the types of policies and authorization methods. The policy ID, sender, recipient, and implementation rules for the policy make up the proposed authorization strategy. The creation of datasets for information for all sensors and users is the initial step in the proposed authorization approach. Policies are established based on prior datasets. Policies on the server are shielded against malicious attacks by using signature-based policy protection. This policy may include a variety of specifications, such as how to choose the day and time of data access, the time limit for a certain day, or the total number of accesses.

- **Requests and responses between sensors/users and servers**

The proposed authorization approach requires sensors and users to create an authorization request before they may access medical records. The sender and receiver details are included in this request. The parameters of the  $SS || Sen_N || Sen_ID$  are used as a piece of single information by the  $Sen_i$  application to create the ECDSA's Signature for the senders and receivers. Additionally, after confirming the Signatures, the  $Sen_i$  application utilizes a portion of the  $Sen_ID$  to explain to the  $BS$  the identification of the entity in order to decide the desired policy. The request is then forwarded by the  $Sen_i$  via the  $BS$  to the  $IS$  for analysis. The request is evaluated by the  $IS$ , and the  $BS$  then provides the result (permit or refuse) to the  $Sen_i$ . In practice, SAML request files are typically generated and managed by the SAML implementation in our proposed approach. They are encoded and transmitted to the destination using the specified binding method, such as a form submission. The process of the request authenticates the sensor/user and generates a SAML response containing the requested assertions and attributes.

- **Utilizing Shamir mechanism**

We adopted the Shamir method to the proposed authorization strategy to boost the security of sensors and users. Due to the privileges assigned to legitimate devices,  $Sen_i$ s are real devices that are capable of posing a risk inside. The proposed authorization approach signs all healthcare sensors' and users' signatures using ECDSA to produce a Shamir secret. Then, the proposed authorization approach creates secrets sharing ( $SS_s$ ) from an  $SS$  using the Shamir manner. The  $SS_i$  is delivered to each network device through a secure communication channel. To rebuild  $SS$ ,  $Sen_i$  needs a collection of  $SS_s$ . Threshold = 3 is used in the proposed authorization strategy, which indicates that the randomly chosen  $SS_s$  need at least 3  $SS_s$  to create  $SS$ . Additionally, based on  $V_i m$ ,  $IS$  identifies the network device as being valid, verifies the original  $SS$  using the Shamir secret and ECDSA's signature, and then assesses the request using security parameters. By combining Shamir's method with SAML, the authenticity feature is added since a  $Sen_i$  cannot access data using the same  $SS_s$ . This procedure makes it possible for the proposed authorization approach to ensure patient data privacy and safeguard patient data from serious threats.

- **Applying encryption on authorization request**

In our protocol, we rely on AES-256 with 10 rounds to mask authorization requests to store health sensor data to protect it from attacks. The use of a symmetric encryption algorithm will enable the health sensors to operate with high performance as well as support the security of network parameters and data collected by the health sensors. Our approach uses AES-256 to protect information signed by ECDSA-Lesamnta-LW and SAML authorization requests.

### 4.3 Proposed authorization approach protocol

This section will go through the proposed authorization protocol framework for authorizing sensors and users in detail. The protocol request contains  $SP$  for a subject (the sender) and an object (the receiver). Figure 8 displays the authorization processing.

- Initially, the  $Sen_i$  device retrieves the  $Sen_{ID}$  and  $BS_{ID}$  identifiers for use in access operations and stores the data collected by the sensors in  $RS$ . Then  $Sen_i$  generates a random number  $Sen_N$ , timestamp ( $TS_i$ ) and uses Shamir secret to produce the original  $SS$ . Next,  $Sen_i/U_i$  performs an electronic signature ( $Sen_S$ ) with  $EC_{LLW}$  to ensure the integrity of the privacy request and based on the  $SS||Sen_N||Sen_{ID}$  security parameters. Then  $Sen_i$  performs the masking of  $TS_i$  and  $BS_{ID}$  in a temporary value of  $V_{tm}$  to prevent information from being leaked. Then  $Sen_i$  uses SAML to generate a privacy request that includes hidden privacy information for the sending and receiving device. Finally,  $Sen_i$  uses AES-192 to protect the SAML request, sign  $Sen_S$ , random number  $Sen_N$  and then transferred the encrypted request  $R_{Sen_1}$  to  $BS$ .
- $BS$  gets the AES-192 encrypted SAML request and performs decryption of the  $R_{BS_1}$  request. Then  $BS_{ID}$  and  $R_{BS_1}$  are used to retrieve the random number  $Sen_N$  which is used with  $Sen_{ID}$  and  $SS$  in signature processing to find  $BS_{S_1}$  and tested with  $Sen_S$  received. After then,  $BS$  verifies  $TS_i$  to check if the request was delivered on time. Next,  $BS$  prepares the SAML authorization request containing  $V_{tm}$  and an electronic signature  $BS_{S_2}$  to be encrypted and sent to the  $IS$  information server.
- $IS$  receives a SAML authorization request containing a  $V_{tm}$  timer value,  $BS_{S_2}$  signature,  $TS_i$  send time, as well as some other  $SP$  security parameters such as  $IS_{ID}$  and  $SS$ .  $IS$  verifies the integrity of the information with  $IS_{S_1}=BS_{S_2}$  and does not delay the authorization request by  $TS_i$ . To authorize the request in  $RS$ ,  $IS$  computes a secret value ( $Sec$ ) which includes  $Sen_{ID}$ ,  $BS_{ID}$ ,  $IS_{ID}$  and  $RS_{ID}$  which is used to authorize requests in the next connections. Similarly,  $IS$  computes the SAML authorization request containing  $V_{tm}$ ,  $IS_{S_2}$  and then  $R_{IS_2}$  encrypts it and sends it to  $RS$  to prove access and store the data collected by  $Sen_i$ .
- At this juncture,  $RS$  gets the SAML authorization message from  $IS$ .  $RS$  validates the SAML request,  $RS_{S_1}$  and  $TS_i$ . If all parameters are valid,  $RS$  allows access or storage of the data collected by  $Sen_i$ , otherwise, it refuses the connection.
- Finally,  $RS$  generates a response request that includes a token accept request ( $T_{AR}$ ) that contains a signature, a random number and the secret value  $Sec$ . Then  $RS$  encrypts the request ( $R_{RS_2}$ ) by  $E_{AES}(T_{AR}||TS_i||RS_{ID})$  and sends it to  $IS$  and then to  $BS$  until it reaches  $Sen_i$  which decrypts the request and verifies the signature and then stores  $Sec$  for next incoming connections.

## 5 Discussions and Security/Performance Analysis

This section investigates an evaluation of theoretical attacks and a security comparison.

### 5.1 Security analysis

By presenting hypotheses and proofs, this section will demonstrate how the proposed approach offers a high level of security against various assaults. Table 5 provides a comparison of privacy properties.

- **Resist against a node outage attack.**

**Proof 1:** This threat entirely disables the operation of any wireless sensor components, including

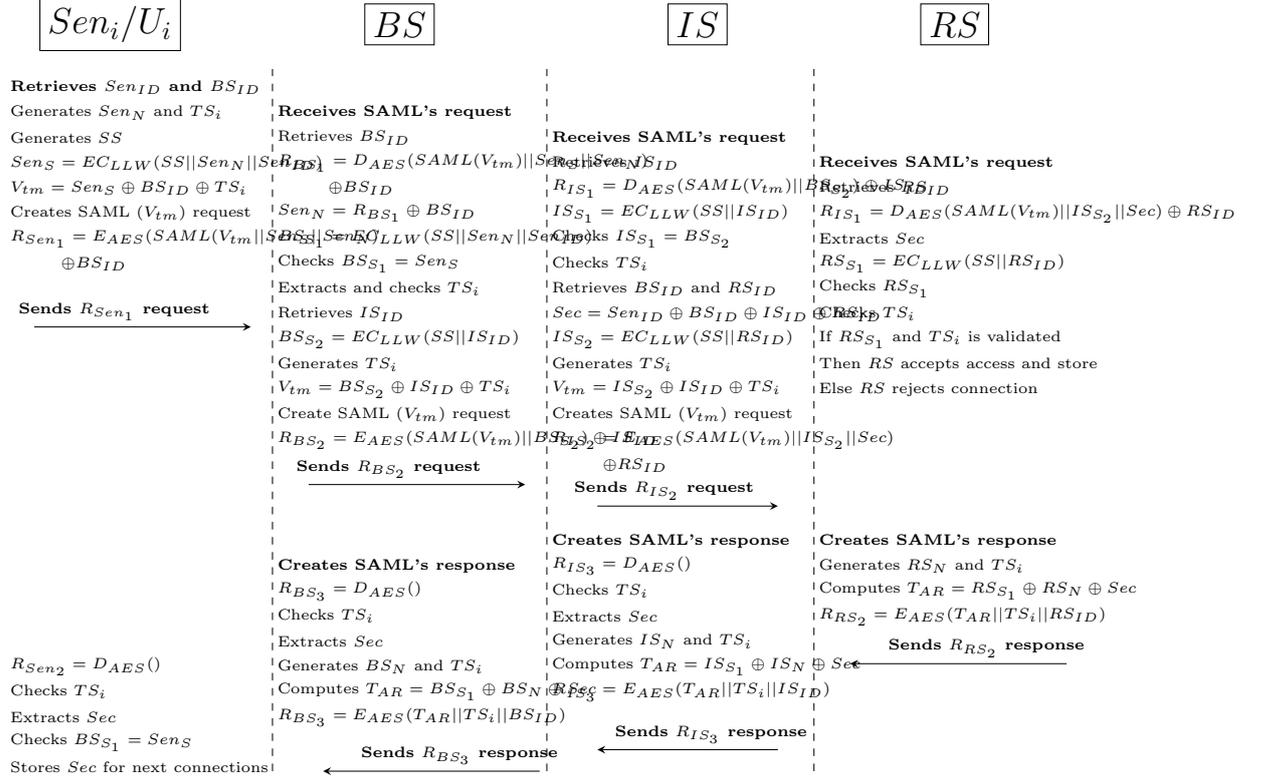


Figure 8: Proposed authorization protocol

sensor nodes, communication links, and master nodes. As a result, the connection to other cluster head nodes located in other areas is severed. The attacker is trying to disconnect a specific  $Sen_i$  or  $Cl_i$ . In our protocol, the data collected by sensors does not depend only on a particular  $Sen_i$  or  $Cl_i$ . Any authorization request that does not contain a valid  $Sen_{ID}$  and  $Sen_N$  is rejected by  $BS$  and  $IS$  servers. This shows that our protocol is resistant to attacks.

- **Resist against the MitM attack.**

**Proof 2:** Consider a scenario in which a hacker tries to intercept encrypted authorization requests from network entities (such  $R_{Sen_1}$ ,  $R_{BS_2}$ , and  $R_{IS_2}$ ) and then replaces or alters this information of requests with his or her own messages to forward to the health sensor network. Nonetheless, the hacker is unable to amend the requests that were sent to  $Sen_i$ ,  $BS$ , and  $IS$  because, first,  $EC_{LLW}$  signatures prohibit  $SP$  from being altered. The alteration of requests between  $Sen_i$ ,  $BS$ ,  $IS$ , and  $RS$  is also prevented by mutual authentication that includes ECDSA-Lesamnta-LW. Consequently, the proposed approach successfully repels the MitM attack.

- **Resist against impersonation attack.**

**Proof 3:** Suppose a hacker impersonates a valid sensor's/user's authorization request in an attempt to get access to the network. Due to the total concealment of the security settings, this hacker is not able to construct  $TS_i$  and  $Sen_N$ . By altering the signatures, the hacker also tries to pass as the  $Sen_i/U_i$  device to access the network. The  $Sen_S$  varies in each connection based on the  $Sen_N$ , rendering this scenario infeasible. As an outcome, our protocol deters threats made in the form of a

Table 5: Comparison of privacy properties

Privacy property	Keerthika and Shanmugapriya [56]	Saini et al. [22]	Chen et al. [23]	Fareed and Yassin [26]	Zala et al. [5]	Office of Information Security [13]	Kumari et al. [57]	Pruthi et al. [58]	Proposed authorization protocol
Anti node outage	✓						✓		✓
Anti MitM		✓	✓	✓	✓				✓
Anti impersonation			✓		✓		✓		✓
Anti rushing	✓			✓			✓		✓
Anti vampire	✓			✓		✓	✓		✓
Anti neglect and greed	✓					✓	✓	✓	✓
Anti packet drop								✓	✓

false identity.

- **Resist against rushing attack.**

**Proof 4:** The hacker breaks down  $Sen_i/U_i$  from the WSN on-demand routings in an effort to make system resources scarce. He/she then swiftly broadcasts bogus route request advertisements across the WSN. As a result, this kind of threat has a major impact on a network connection and degrades networking capabilities including message delivery and control. The malicious device rushes to transfer the messages from the neighbor to the other destination sensor through a separate tunnel. Our protocol provides a countermeasure of this threat is that entities such as  $(Sen_i, Cl_i, BS, IS$  and  $RS)$  do not allow the connection to be accepted until all security parameters in  $V_{tm}$  are met, the hacker cannot change the routing path. Therefore, our approach resists this onslaught.

- **Resist against vampire attack.**

**Proof 5:** This threat is the type of denial of service (DoS) threat that consumes the energy of  $Sen_i$  and completely declines the network. It employs the sending of a request that utilizes more network energy than a legitimate  $Sen_i$  would if it sent data of a similar size to the same destination. Also, Vampires use protocol-compliant data. To counteract the vampire, our protocol introduces authentication and verification (such as  $SS$  and  $TS_i$ ) before accepting authorization requests and prevents heavy repetitive (infinitely looped) transfers from a given entity.

- **Resist against neglect and greed attack.**

**Proof 6:** By delivering the request to the incorrect sensor, the hacker chooses the longest route to convey the information. The unauthorized  $Sen_i$  neglects to transfer the information and drops them randomly. Instead, hacker becomes greedy and transfer their own information to the other sensors. This behavior will reduce the remaining energy of the sensors found in that path, thus breakdown the health sensor network quickly. Our approach uses authorization mechanisms (such as SAML authorization) to limit and detect this type of attack both between sensor nodes and all network entities.

- **Resist against packet drop attack.**

**Proof 7:** Launching a packet-dropping threat is for a malicious sensor to get involved during path formation. This is exploiting the vulnerabilities of the routing protocols utilized in health sensors which are designed based on the assumption of trustworthiness between sensors in a network. This type of attack can cause packets not to arrive in a timely manner or not to receive a response to authorization requests from entities. Our approach uses  $TS_i$  to make sure authorization requests arrive in a timely manner. Also, any authorization request that does not contain  $Sec$  or that does not reach the target destination indicates that the authorization request has been subjected to a drop packet attack. Therefore, our protocol detects and mitigates the risk of this attack.

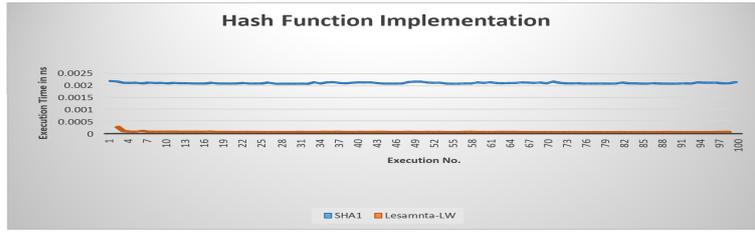


Figure 9: Comparison between SHA1 and Lesamnta-LW



Figure 10: Comparison between ECDSA-SHA1 and ECDSA-Lesamnta-LW

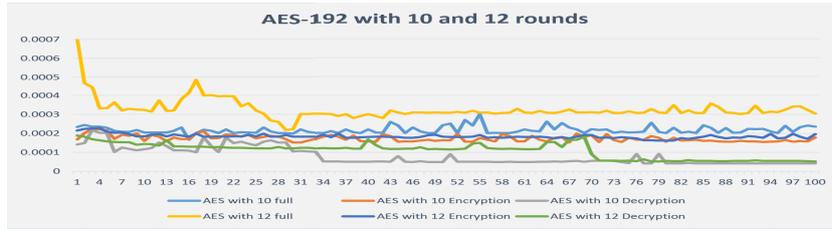


Figure 11: Performance comparison between AES with 10 rounds and AES with 12 rounds

## 5.2 Performance analysis

This section describes how the proposed protocol performs in a scenario with health sensors. It offers evaluations for the 256-bit Lesamnta-LW hash function, 256-bit ECDSA signature technique, and 192-bit AES encryption cryptography. To determine the effectiveness of the proposed strategy, communication costs (storage overheads) and computation (execution time) are also considered. C programming language is used to create the application codes  $Sen_i$ ,  $BS$ ,  $IS$ , and  $RS$ . The findings are also applied with Ubuntu 20.04 LTS, an Intel Core i5 CPU running at 2.6GHz, a 64-bit operating system, 16 GiB of memory, and a 32.0 GB hard drive. Our protocol performs best as can be seen in Figure 9 which shows Lesamnta-LW outperforming SHA1. Also, Figure 10 shows the superior performance of ECDSA-Lesamnta-LW over ECDSA-SHA1. Finally, Figure 11 shows that AES 192 bits with 10 rounds performs better than AES with 12 rounds. Table 6 compares performance of computation cost our protocol with existing protocols (where the time complexity of the hash function is  $T_h$ ).

## 6 Conclusion

One fundamental need for sensor health systems is the security of sensor data. The accuracy and safety of patients' lives depend heavily on the safeguarding of this sensitive data. Therefore, we suggested a privacy

Table 6: Comparison of computation cost between authorization protocols

Protocol	Hashes on $Sen_i$	Hashes on $BS$	Total	Hash class	Encryption type	Execution time in ms	Requests No.	Bits No.
Ghani et al. [59]	$1T_h$	$2T_h$	$3T_h$	Standard	Symmetric	0.0207	6	1344
Gope et al. [60]	$4T_h$	$9T_h$	$13T_h$	Standard	-	10.8	6	704
Das et al. [61]	$3T_h$	$7T_h$	$10T_h$	Standard	-	$0.0001+0.442$	4	768
<b>Proposed</b>	$1T_h$	$2T_h$	$3T_h$	Lightweight	AES-192	0.002358	6	253

protocol that was primarily based on Shamir, ECDSA, SAML, and AES-192. We have demonstrated through the evaluation results that our protocol can prevent attacks on this search field and provides superior performance over the current search performance. Future trends include expanding security (to include additional assaults), performance testing with more performance metrics, and apps in various health settings.

## References

- [1] M. Al-Zubaidie and R. A. Muhajjar, "Integrating trustworthy mechanisms to support data and information security in health sensors," *Procedia Computer Science*, vol. 237, pp. 43–52, 2024. [Online]. Available: <https://doi.org/10.1016/j.procs.2024.05.078>
- [2] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," *Future Internet*, vol. 15, no. 8, p. 262, 2023. [Online]. Available: <https://doi.org/10.3390/fi15080262>
- [3] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted ehr sharing with security and privacy preservation via consortium blockchain," *Ieee Access*, vol. 7, pp. 136 704–136 719, 2019.
- [4] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Informatics Journal*, vol. 20, no. 2, pp. 97–108, 2019.
- [5] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "PRMS: Design and development of patients' e-healthcare records management system for privacy preservation in third party cloud platforms," *IEEE Access*, vol. 10, pp. 85 777–85 791, 2022.
- [6] P. K. D. Pramanik, G. Pareek, and A. Nayyar, "Security and privacy in remote healthcare: Issues, solutions, and standards," in *Telemedicine technologies*. Elsevier, 2019, pp. 201–225.
- [7] M. Al-Zubaidie and W. A. Jebbar, "Providing security for flash loan system using cryptocurrency wallets supported by xsalsa20 in a blockchain environment," *Applied Sciences*, vol. 14, no. 14, p. 6361, 2024. [Online]. Available: <https://doi.org/10.3390/app14146361>
- [8] L. Irwin, "Data breaches and cyber attacks quarterly review: Q2 2021," July 2021. [Online]. Available: <https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-quarterly-review-q2-2021>
- [9] D. H. Tahayur and M. Al-Zubaidie, "Establishing an optimized searching approach with e-signatures based on blockchain for electronic agriculture applications," in *AIP Conference Proceedings*, vol. 3264, no. 1. AIP Publishing LLC, 2025, p. 030001. [Online]. Available: <https://doi.org/10.1063/5.0258784>
- [10] R. H. Razzaq, M. Al-Zubaidie, and R. G. Atiyah, "Intermediary decentralized computing and private blockchain mechanisms for privacy preservation in the internet of medical things," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp. 152–165, 2024. [Online]. Available: <https://doi.org/10.58496/MJCS/2024/020>
- [11] R. H. Razzaq and M. H. Al-Zubaidie, "Maintaining security of patient data by employing private blockchain and fog computing technologies based on internet of medical things," *Informatika*, vol. 48, no. 12, 2024. [Online]. Available: <https://doi.org/10.31449/inf.v48i12.6047>
- [12] M. Maskun, R. Nugraha, H. Assidiq, M. Tayyib, and A. Syafira, "Harmonization over the regulations of electronic medical records and its potential to be abused," *Medico-legal Update*, vol. 21, no. 1, 2021.
- [13] Office of Information Security, "Web application attacks in healthcare," Health Sector Cybersecurity Coordination Center, Tech. Rep., July 21, 2022, viewed 05 September 2022, <https://www.hhs.gov/sites/default/files/web-application-attacks-in-healthcare.pdf>.

- [14] J. Davis, "Hhs alerts to ongoing healthcare web app attacks, urges review of tactics," Tech. Rep., July 25, 2022, viewed 06 September 2022, <https://www.scmagazine.com/analysis/application-security/hhs-alerts-to-ongoing-healthcare-web-app-attacks-urges-review-of-tactics>.
- [15] Awaad, Mishall Hammed, "Improve the effectiveness of sensor networks and extend the network lifetime using 2BSs and determination of area of CHs choice," *Journal of Computer Science and Control Systems*, vol. 7, no. 1, p. 15, 2014.
- [16] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.
- [17] W. A. Jebbar and M. Al-Zubaidie, "Transaction-based blockchain systems security improvement employing micro-segmentation controlled by smart contracts and detection of saddle Goatfish," *SN Computer Science*, vol. 5, no. 7, p. 898, 2024. [Online]. Available: <https://doi.org/10.1007/s42979-024-03239-9>
- [18] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for xml-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.
- [19] G. S. Shyaa and M. Al-Zubaidie, "Securing transactions using hybrid cryptography in e-commerce apps," *Journal of Education for Pure Science-University of Thi-Qar*, vol. 13, no. 3, pp. 27–52, 2023.
- [20] G. S. Shyaa and M. Al-Zubaidie, "Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography," *Applied Sciences*, vol. 13, no. 12, p. 7085, 2023. [Online]. Available: <https://doi.org/10.3390/app13127085>
- [21] E. Zaghoul, T. Li, and J. Ren, "Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts," in *2019 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2019, pp. 375–379.
- [22] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5914–5925, 2020.
- [23] C.-L. Chen, P.-T. Huang, Y.-Y. Deng, H.-C. Chen, and Y.-C. Wang, "A secure electronic medical record authorization system for smart device application in cloud computing environments," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–31, 2020.
- [24] H. Wu, A. D. Dwivedi, and G. Srivastava, "Security and privacy of patient information in medical systems based on blockchain technology," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 17, no. 2s, pp. 1–17, 2021.
- [25] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, "Secure decentralized electronic health records sharing system based on blockchains," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5045–5058, 2022.
- [26] M. Fareed and A. A. Yassin, "Privacy-preserving multi-factor authentication and role-based access control scheme for the e-healthcare system," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 2131–2141, 2022.
- [27] R. H. Razzaq and M. Al-Zubaidie, "Formulating an advanced security protocol for internet of medical things based on blockchain and fog computing technologies," *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 3, pp. 723–734, 2024. [Online]. Available: <https://doi.org/10.30880/ijcsm.2024.05.03.046>
- [28] P. Visconti, S. Capoccia, E. Venere, R. Velázquez, and R. d. Fazio, "10 clock-periods pipelined implementation of aes-128 encryption-decryption algorithm up to 28 gbit/s real throughput by xilinx zynq ultrascale+ mpoc zcu102 platform," *Electronics*, vol. 9, no. 10, p. 1665, 2020.
- [29] W. A. Jebbar, R. H. Razzaq, D. H. Tahayur, and M. Al-Zubaidie, "Blockchain and cryptography framework of e-apps with big data," *Journal of Education for Pure Science-University of Thi-Qar*, vol. 14, no. 3, 2024. [Online]. Available: <https://doi.org/10.32792/jeps.v14i3.545>
- [30] M. H. Al-Zubaidie and R. H. Razzaq, "Combining fog computing and blockchain based on the internet of medical things to preserve patient information privacy," in *Sustainable Information Security in the Age of AI and Green Computing*. IGI Global Scientific Publishing, 2025, pp. 525–546. [Online]. Available: <https://doi.org/10.4018/979-8-3693-8034-5.ch026>

- [31] T. G. Tregi and M. Al-Zubaidie, "Enhancing traffic data security in smart cities using optimized quantum-based digital signatures and privacy-preserving techniques," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 256–272, 2025. [Online]. Available: <https://doi.org/10.58496/MJCS/2025/017>
- [32] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system," *International Journal of Environmental Research and Public Health*, vol. 16, no. 9, p. 1490, 2019. [Online]. Available: <https://doi.org/10.3390/ijerph16091490>
- [33] W. J. Buchanan, "Elliptic curve digital signature algorithm (ecdsa)," <https://asecuritysite.com/signatures/ecdsa2>, Asecuritysite.com, 2022, accessed: September 14, 2022. [Online]. Available: <https://asecuritysite.com/signatures/ecdsa2>
- [34] M. H. Awaad and W. A. Jebbar, "Extending the WSN lifetime by dividing the network area into a specific zones," *International Journal of Computer Network and Information Security*, vol. 7, no. 2, pp. 33–39, 2015.
- [35] D. Tahayur, W. Jebbar, R. Razzaq, and M. Al-Zubaidie, "Dependable concealing algorithm of e-apps repositories combined with a robust blockchain approach," *Advanced Research on Information Systems Security, an International Journal*, vol. 4, no. 2, pp. 32–56, 2024. [Online]. Available: <https://doi.org/10.56394/aris2.v4i2.48>
- [36] M. H. Awaad and W. A. Jebbar, "Prolong the lifetime of WSN by determining a correlation nodes in the same zone and searching for the best not the closest CH," *International Journal of Modern Education and Computer Science*, vol. 6, no. 11, p. 31, 2014.
- [37] D. H. Tahayur and M. Al-Zubaidie, "Enhancing electronic agriculture data security with a blockchain-based search method and e-signatures," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp. 1–21, 2024. [Online]. Available: <https://doi.org/10.58496/MJCS/2024/012>
- [38] R. H. Razzaq, D. H. Tahayur, W. A. Jebbar, and M. Al-Zubaidie, "Sturdy blockchain combined with e-apps repositories based on reliable camouflaging and integrating mechanisms," *I. J. Computer Network and Information Security*, vol. 17, no. 3, pp. 35–53, 2025. [Online]. Available: <https://doi.org/10.5815/ijcnis.2025.03.03>
- [39] N. F. Syed, S. W. Shah, A. Shaghghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57 143–57 179, 2022.
- [40] M. H. Al-Zubaidie and D. H. Tahayur, "Security cooperation in the protection concerns of agriculture data using efficient signatures and artificial bee colony manner," in *Sustainable Information Security in the Age of AI and Green Computing*. IGI Global Scientific Publishing, 2025, pp. 439–460. [Online]. Available: <https://doi.org/10.4018/979-8-3693-8034-5.ch022>
- [41] N. Nabeel, M. Habaebi, N. C. Mustapha, and R. Islam, "Iot light weight (lwt) crypto functions," vol. 13, pp. 117–129, 2019.
- [42] M. H. Awaad and W. A. Jebbar, "Study to analyze and compare the LEACH protocol with three methods to improve it and determine the best choice," *Journal of Computer Science and Control Systems*, vol. 7, no. 2, p. 5, 2014.
- [43] A. F. Marhoon and M. H. Awaad, "Reduce energy consumption by improving the LEACH protocol," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 1, pp. 01–09, 2014.
- [44] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, and H. Yoshida, "A lightweight 256-bit hash function for hardware and low-end devices: Lesamnta-lw," in *International Conference on Information Security and Cryptology*. Springer, 2010, pp. 151–168.
- [45] A. Mileva, V. Dimitrova, O. Kara, and M. J. Mihaljević, "Catalog and illustrative examples of lightweight cryptographic primitives," in *Security of Ubiquitous Computing Systems*. Springer, 2021, pp. 21–47.
- [46] M. Al-Zubaidie, R. A. Muhajjar, and L. A. Shihabe, "Computer networking and cloud-based learning/teaching environment using virtual labs tools: A review and future aspirations," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 176–203, 2024. [Online]. Available: <https://doi.org/10.58496/MJCS/2024/015>

- [47] R. Kumar and N. Agrawal, "Rbac-lbrm: An rbac-based load balancing assisted efficient resource management framework for iot-edge-fog network," *IEEE Sensors Letters*, vol. 6, no. 8, pp. 1–4, 2022.
- [48] A. Biswas, G. Baranwal, and A. K. Tripathi, "Abac: Alternative by alternative comparison based multi-criteria decision making method," *Expert Systems with Applications*, vol. 208, p. 118174, 2022.
- [49] C. Caserio, F. Lonetti, and E. Marchetti, "A formal validation approach for xacml 3.0 access control policy," *Sensors*, vol. 22, no. 8, p. 2984, 2022.
- [50] F. Deng, Z. Yu, H. Song, L. Zhang, X. Song, M. Zhang, Z. Zhang, and Y. Mei, "Improvement on pdp evaluation performance based on neural networks and sgdk-means algorithm," *Soft Computing*, vol. 26, no. 6, pp. 3075–3089, 2022.
- [51] Z. Yu, Y. Yan, F. Deng, F. Zhang, and Z. Li, "An efficient density peak cluster algorithm for improving policy evaluation performance," *Scientific Reports*, vol. 12, no. 1, pp. 1–19, 2022.
- [52] M. H. Al-Zubaidie and W. A. Jebbar, "Optimization solution proposal for smart transaction security of smart blockchain contracts in e-banking applications," in *Sustainable Information Security in the Age of AI and Green Computing*. IGI Global Scientific Publishing, 2025, pp. 295–320. [Online]. Available: <https://doi.org/10.4018/979-8-3693-8034-5.ch015>
- [53] H. K. Maji, H. H. Nguyen, A. Paskin-Cherniavsky, and M. Wang, "Improved bound on the local leakage-resilience of shamir's secret sharing," in *2022 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2022, pp. 2678–2683.
- [54] A. Hineman and M. Blaum, "A modified shamir secret sharing scheme with efficient encoding," *IEEE Communications Letters*, vol. 26, no. 4, pp. 758–762, 2022.
- [55] S. A. Abdel Hakeem and H. Kim, "Centralized threshold key generation protocol based on shamir secret sharing and hmac authentication," *Sensors*, vol. 22, no. 1, p. 331, 2022.
- [56] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362–367, 2021.
- [57] S. Kumari, K. K. Singh, P. Nand, G. S. Mishra, and R. Astya, "A comparative study of security issues and attacks on underwater sensor network," in *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021*. Springer, 2022, pp. 59–74.
- [58] V. Pruthi, K. Mittal, N. Sharma, and I. Kaushik, "Network layers threats & its countermeasures in WSNs," in *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 2019, pp. 156–163.
- [59] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in iot-based wireless sensor networks: An authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, p. e4139, 2019.
- [60] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE transactions on industrial informatics*, vol. 15, no. 9, pp. 4957–4968, 2019.
- [61] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1899–1933, 2017.