PRIVACY-PRESERVING MEDICAL RECORD SEARCHING SCHEME (PMRSS) FOR IOT HEALTHCARE

[#1]NALLA SAITEJA,

[#2]B.ANVESH KUMAR, *Assistant Professor,*

[#3]Dr.V.BAPUJI, *Associate Professor& HOD,*

Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

ABSTRACT: One field that makes use of IoT technology is healthcare, where sensors and IoT-enabled medical devices send data to professionals without the need for human intervention. Prior patients' medical records are extremely private, but they are essential in assisting current patients in diagnosing their ailment. As a result, it is critical to make the best use of patient records while protecting their privacy. In this study, a novel Self Diagnosis Platform (SDP) is created that securely extracts patient records from earlier records without jeopardizing either the patient's or the record database's privacy. The patient's device first collects data from sensors implanted in the patient's body, which is then encrypted with Edwards' Digital Signature Algorithm. The data is then encrypted and forwarded to the Secure Disease Archive (SDA), which stores earlier data. Similar records will be obtained from the database via the SDP based on the patient's data. In terms of encryption time, execution time, and end-to-end delay, the proposed framework is compared to existing solutions. The recommended SDP strategy outperforms the LDQN, SE-AC, PMDA, and EPPDA techniques by 30.63%, 27.48%, 22.07%, and 9.23%, respectively. For real-time applications, this strategy is more efficient and secure.

Keywords: Internet of things, Self-diagnosis platform, Security, Edward's digital signature algorithm, Encryption, Decryption.

1. INTRODUCTION

The term "Internet of Things" (IoT) is used to describe a system in which every component is connected to the internet, allowing for remote access from anywhere at any time. The impact of the Internet of Things (IoT) is felt strongly in the technical and social spheres. The Internet of Things (IoT) is used in a wide range of industries, including but not limited to healthcare, mining, building construction, agriculture, transportation, and others.

Internet of Things (IoT) applications in healthcare have shown great promise. Accessibility, proactivity, and individualization in healthcare are all areas where the Internet of Things (IoT) can be used to make a difference for patients. The Internet of Things (IoT) is a paradigm that incorporates many components such as sensors and actuators for the creation of medical devices, and it is inextricably linked to the integration of image processing algorithms. The present focus of healthcare professionals is on enhancing the quality of interactions between patients and healthcare institutions to better ensure patients' well-being.

When applied to the healthcare industry, IoT technology not only improves patients' well-being but also allows for timely monitoring of their status from a remote place, allowing for fast emergency response if necessary. Remote monitoring of the elderly, those in long-term care facilities, and people with mobility restrictions are only some of the scenarios illustrated. Other types of monitoring, such as "effective monitoring," "monitoring of specific patient conditions," and "monitoring of patient mobility," are also included.

The helpful data can be used to create smart apps like e-Doctor sites, medicine suggestion systems, and self-diagnosis platforms, among many others.

In the context of solving a health problem, the use of an online platform for self-diagnosis has the potential to increase patient satisfaction and perceived service quality while decreasing provider costs. Incredibly complex challenges lie ahead in the form of a self-diagnosis platform's development. The system's accuracy is a source of worry, among others. Correctly diagnosing an illness requires a comprehensive process that takes into account a wide range of factors. Several attempts have been made to create this kind of system. Nonetheless, the vast majority of these have not been put into action.

Health companies around the world have benefited from a more user-centric, structured, and productive environment as a direct result of adopting a multimedia approach. Large data stores create security concerns and often necessitate human intervention. Smart healthcare apps must use safe data transmission protocols to protect patients' personal information from hackers and other security risks. The following is the primary goal of the proposed framework.

It is recommended to think about implementing a Secure Diagnostic Platform (SDP) that protects patient data and keeps people's privacy intact when they go through diagnostic procedures.

The Edwards Curve Digital Signature Algorithm is used to encrypt the patient data collected by sensors.

The Secure Disease Archive (SDA) is in charge of data collection and storage. The proposed SDP architecture uses encryption methods to safeguard private patient information.

2. LITERATURE REVIEW

The possible implications of disclosing a patient's personal information can be damaging to their personal and professional lives, underscoring the necessity of maintaining patient confidentiality. Researchers in the past have used cryptography technologies extensively to solve this problem. There are many topics that could be discussed, but only a few that fit within the confines of this article.

Yang (2018) presented a novel electronic health record system with the intention of protecting patient confidentiality. The cloud, IoT, and big data are all brought together in this synthesis. Using keyword matches to update policy allows for flexible policy changes that still maintain privacy rules. Simulations and comparisons have shown the efficacy of the system-provided algorithms.

To reduce the computational burden of protecting against intermediary attacks, Mohamed Shakeel, in 2018, created a Deep-Q-Networks (LDQN) that makes use of several learning approaches. The suggested approach employs the Q-learning framework to perform a hierarchical analysis of medical data. Therefore, with its error rate being only 12%, the LDQN method is able to correctly identify 98.79% of malware cases.

Liu presented the Blockchain-based Electronic Medical Record Data Sharing (BPDS) system in 2018 with the intention of protecting patient information. Cloud-based storage for EMRs and the storage of indexes on an immutable consortium blockchain ensure that the use of centralized storage is not a security risk in the context of BPDS. The proposed Blockchain-based Patient Data System (BPDS) will allow consumers and organizations to securely and effectively access patient data. Patients will also have the independence to manage their own EMRs (Electronic Medical Records).

In 2019, Liu, X. created a solution to improve the electronic health system by facilitating the sharing and preservation of clinical data through the use of a private blockchain infrastructure within a hospital context. This investigation makes use of the Open SSL cryptography library and a Public Key Cryptography (PBC) system as its technique. According to the results, the proposed technique efficiently satisfies many criteria while reducing the load on both computing and communication infrastructure.

To better manage electronic health records (EHRs) stored in the cloud and to allow for more accurate access control in crisis situations, Riad in 2019 created the sensitive and energetic access control (SE-AC) mechanism. The SE-AC technique permits the use of several concurrent operations to boost execution performance. The

results of the performance analysis show that the proposed approach is viable in a variety of contexts, including IoT healthcare systems.

N. Chikouche presented a new method of authentication for IoT devices in 2019 that uses a cryptographic key code to protect user anonymity. One of the most important forms of post-quantum encryption that can withstand quantum attacks is code-based cryptography. The proposed protocol has been found to outperform state-of-the-art methods in terms of security and efficiency, according to empirical studies.

Using blockchain technology, Rajawat (2021) presented a method that gives importance to a number of crucial characteristics, such as completeness, verifiability, suitability, resistance to coercion, resilience, and novelty. The implementation also used a consensus mechanism and the SHA256 hashing algorithm. In addition, the method was used in real-time to protect medical datasets, regardless of the capacity or scalability of the storage media.

A new method of secure data sharing and exchange (DSSE) for IIoT systems was presented in 2021 by Liu et al. The approach was developed with the goal of keeping individuals' private health information safe. Aspect access control is a feature built into the proposed system that grants users varied degrees of access to attribute values. Experiments and in-depth security assessments have shown that the proposed paradigm works and is safe to use.

Within the framework of the Internet of Things (IoT), Peng et al. devised a privacy-preserving multidimensional data aggregation approach (PMDA) in 2021. In this method, a multidimensional vector of small integers is encrypted using a technique based on the Chinese remainder theorem. The encryption method makes use of dimension-dependent linear homomorphic features. The proposed method outperforms the current system in terms of processing and communication costs while still meeting all of the specified security criteria.

The Efficient and Privacy-Preserving Data Aggregation (EPPDA) approach, developed by Almalki and Soufiene in 2021, makes use of IoT authentication to solve problems in the healthcare industry. During both the authorizing and verifying phases, the EPPDA (Eligibility-based Participant Node Aggregation) system evaluates the eligibility of individual nodes to carry out aggregation activities. When tested on low-powered devices, the proposed approach outperforms the state-of-the-art alternatives.

Azeem, M. presented the ESDTA (efficient and secure data transmission and aggregation) method in 2021 with the intention of enhancing the safety and effectiveness of such procedures. Data aggregation utilizing delimiters is the topic of this research, which looks at this process in the context of data compiled from multiple sources. The simulation results show that the transmission and communication costs can be reduced by pooling MN (Mobile Node) resources.

The PMRSS was created by Sun, Y. in 2021 to anonymously analyze medical records. This procedure enabled two iterations of conversation over the diagnostic report without disclosing any supplementary individual data. The technique dramatically improves data collection rates and is well suited to the requirements of 5G's lightning-fast data transfers.

The aforementioned approaches have limitations, such as high costs, a lack of consideration for different kinds of health data, and an inability to guarantee bidirectional security for IoT in healthcare. The proposed method of Software-Defined Perimeter (SDP) successfully mitigates and eliminates these constraints by establishing robust security mechanisms. The System Development Process (SDP) is described in the next section.

3. SYSTEM MODEL

The Self Diagnosis Platform (SDP) architecture is discussed here. The Edwards Curve Digital Signature Algorithm is used by sensors to digitally sign sensitive patient data before sending it to the Secure Disease Archive (SDA). Patient data is kept confidential in the proposed SDP framework due to the usage of encryption. In Figure 1, we see a block representation of the SDP's internal structure.

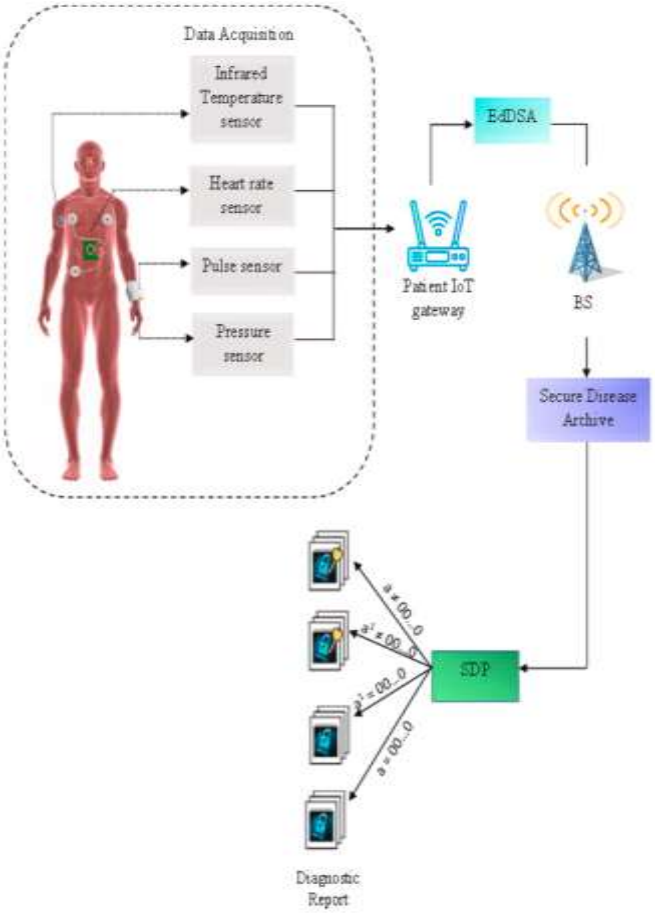


Fig. 1. The proposed SDP framework for preserving medical data

EdDSA algorithm

An example of a cryptographic signature technique that manages to be both secure and easy to implement in software is the Edwards-curve Digital Signature Algorithm (EdDSA). Strong security, effective use of storage resources, and quick signature creation and verification are three of EdDSA's key benefits.

Secure Disease Archive

The Secure Disease Archive (SDA) is a mechanism for safeguarding delayed release archives that takes into account both legal and technical considerations. In order to prevent data breaches, technological issues, and legal processes, SDA employs cutting-edge cryptography and institutional contracts to monitor who has access to whose archives.Using SDA to prevent premature archival data sharing via this distributed security architecture is considerably more difficult.

Self-diagnosis platform

We'll break down the three stages that make up the proposed self-diagnosis platform: inquiry, collation, and retrieval.

Inquiry phase

After collecting patient information, sensors encrypt it with the EdDSA cryptographic technique before sending it across the gateway to the Secure Data Aggregator (SDA). Using the information gathered from the patient's device, we can zero in on the diseases of interest to the patient while ruling out others. In addition, the diagnostic criteria used by doctors are explained to the patient.

4. SYSTEM ANALYSIS

MATLAB2019b was used to create the experimental environment for the proposed semi definite programming (SDP). In order to evaluate the efficacy of the proposed SDP framework, this part provides a comparative analysis of its performance in respect to other methods, including LDQN, SE-AC, PMDA, and EPPDA. Table 2 displays the simulation parameters necessary for the investigation.

Parameters	Value
No. of nodes	15 RAM
Supply voltage	1.9V
Size of packet	4000 bits
Sensor energy	0.5J
Constant bit rate	243 kbps

Fig:2 In this declaration, the proposed Secure Data Protection (SDP) framework's security is analyzed for several key sizes (256 bits, 128 bits, 112 bits, and 80 bits). By using larger keys, the proposed system's security is improved.

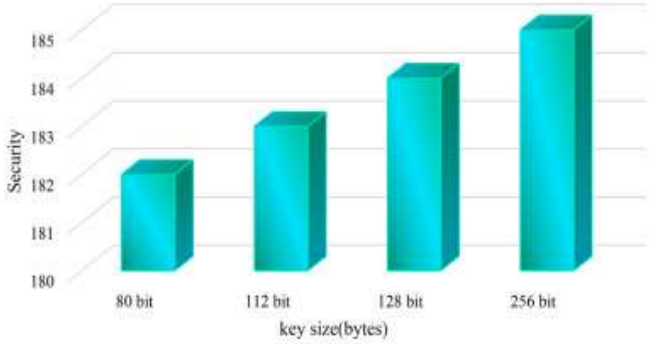
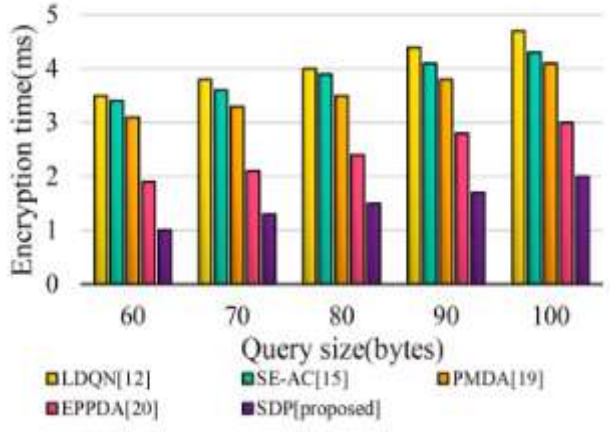
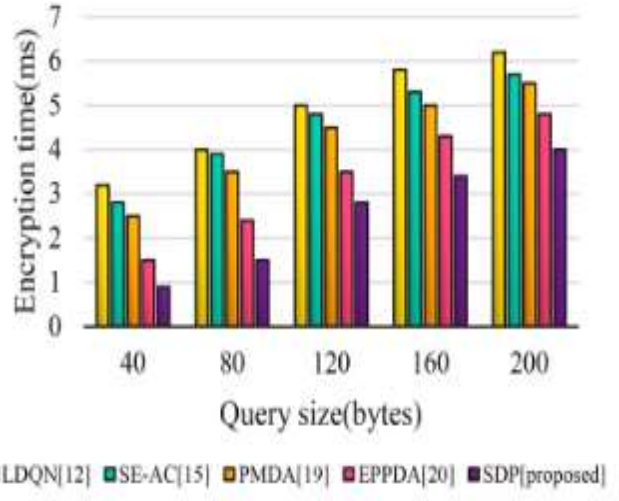


Fig. 2. Security level with respect to key size.

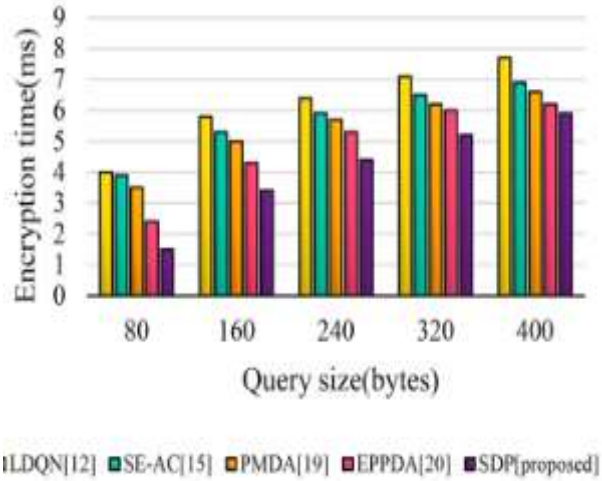
Figure 3 displays the results showing that the proposed method outperforms LDQN, SE-AC, PMDA, and EPPDA when it comes to data encryption efficiency. Encryption time is thus determined by a series of queries, each of which can be no more than 400 bytes in length. The proposed solution outperforms currently used encryption techniques in terms of encryption rate.



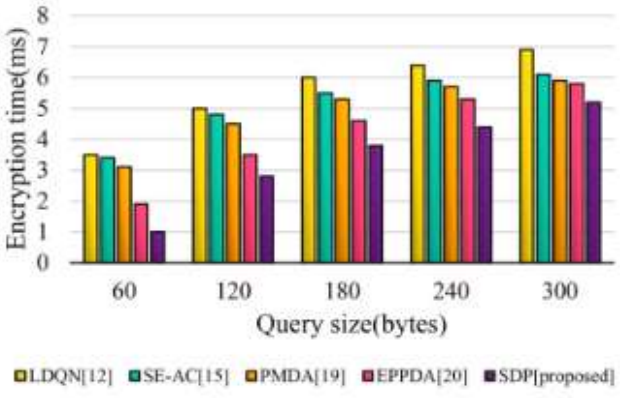
(i) When Query size = 100



(ii) When Query size = 200



(iii)When Query size = 300

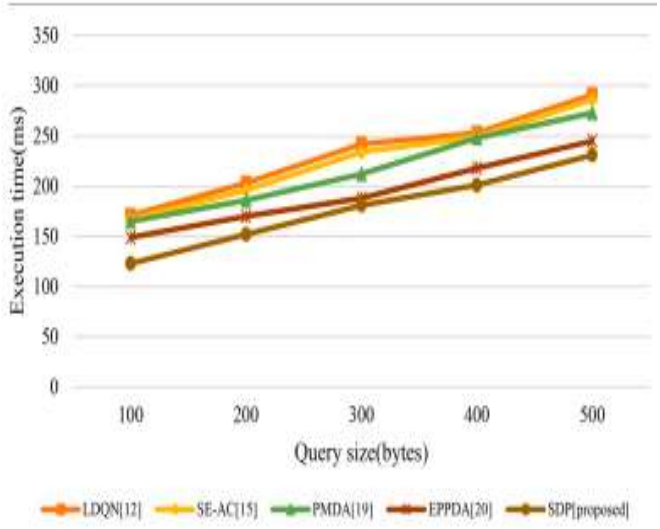


(iv) When Query size = 400

The time it takes to encrypt varies depending on the amount and number of queries, as shown in Figure 3.

The length of time it takes to complete a query varies with its magnitude, as seen in Figure 4.

Here, we examine and contrast the LDQN [12], SE-AC [15], PMDA [19], and EPPDA [20] techniques. The time required to run is proportional to the length of the query. The proposed SDP architecture reduces execution times by 30.63, 27.48, 22.0, and 9.23% compared to the LDQN, SE-AC, PMDA, and EPPDA approaches, respectively.



In Figure 4, we see a graph depicting the correlation between processing time and query size.

Delay in a system as a function of sensor count is depicted in Fig. 5. End-to-end delay decreases as the number of monitors is reduced. The proposed SDP architecture decreases end-to-end delay by 65.5%, 50.6%, 34.85%, and 12.86% when compared to the LDQN, SE-AC, PMDA, and EPPDA methods, respectively..

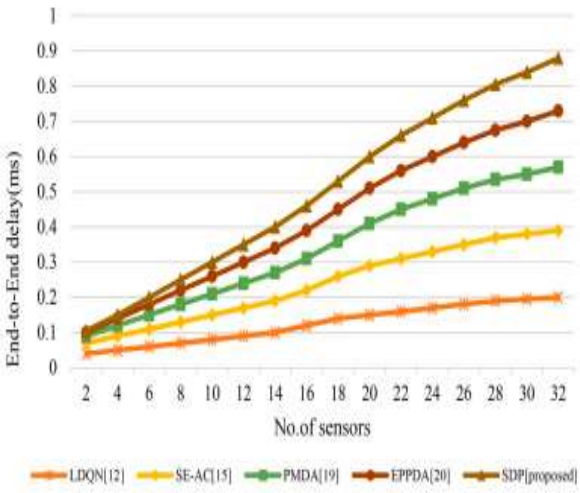


Fig. 5. Comparison with End-to-End delay.

5. CONCLUSION

This research presents a new way of thinking about the Internet of Things (IoT) in healthcare; it's termed the Self-diagnosis Platform (SDP). The use of EdDSA encryption in this method increases privacy by ensuring that neither the patient's nor the third party's identities are revealed to the other. In real-world settings, SDP has proven its efficacy and adaptability. The proposed protocol outperforms established methods like LDQN, SE-AC, PMDA, and EPPDA in terms of encryption time, end-to-end latency, and execution time, according to experimental results. With improvements of 30.63 percent, 27.48 percent, 22.0 percent, and 9.23 percent in execution time and 65.55 percent, 50.62 percent, 34.85 percent, and 12.8 percent in end-to-end latency, respectively, the SDP technique outperforms LDQN, SE-AC, PMDA, and EPPDA. It is hoped that the SDP database will be optimized and compressed in the future, while standardized patient criteria are also established at the same time. Execution of the proposed approaches on real-world systems is crucial for validating the stated findings.

REFERENCES

1. D.A. Gandhi, M. Ghosal Intelligent healthcare using IoT: a extensive survey 2018 Second International Co*nference on Inventive Communication and Computational Technologies (ICICCT)*, IEEE (2018, April), pp. 800-802

2.F. Hussain, S.G. Abbas, G.A. Shah, I.M. Pires, U.U. Fayyaz, F. Shahzad, N.M. Garcia, E. Zdravevski A framework for malicious traffic detection in IoT healthcare environment Sensors, 21 (9) (2021), p. 3025

3.A. Ullah, M. Azeem, H. Ashraf, A.A. Alaboudi, M. Humayun, N.Z. Jhanjhi Secure healthcare data aggregation and transmission in IoT—a survey IEEE Access, 9 (2021), pp. 16849-16865

4. T. Alladi, V. Chamola HARCI: a two-way authentication protocol for three entityhealthcare IoT networks IEEE J. Sel. Area. Commun., 39 (2) (2020), pp. 361-369

5. N. Bilandi, H.K. Verma, R. Dhir Energy-efficient relay node selection scheme for sustainable wireless body area networks Sustain.

Comput.: Informat. Syst., 30 (2021), Article 100516

6. Q. Liu, K.G. Mkongwa, C. Zhang Performance issues in wireless body area networks for the healthcare application: a survey and future prospects SN Appl. Sci., 3 (2) (2021), pp. 1-19

7. N. Ahmad, R.P. George, R. Jahan Emerging trends in IoT for categorized health care 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), vol. 1, IEEE (2019, July), pp. 1438-1441