Internet of Things Protocols for Context-Aware Anonymity Authentication with an Emphasis on E-Health Applications

Shipra Srivastava
Greater Noida
Institute of Technology,
Greater Noida, U.P., India
shiprasrivastava2000@gmail.com

Sumeet Gupta
School of Business, UPES
sumeetgupta@ddn.upes.ac.in

Anita Gehlot
Uttaranchal Institute of Technology,
Uttaranchal University, India
dranitagehlot@gmail.com

Pradkhshana Vijay
Department of Oral Pathology and Microbiology, FODS,
King George's Medical University,
Lucknow , Uttar Pradesh, India
vijaydhar38@yahoo.in

Garla Ramesh
Electronics and Communication Engineering
St.Martins Engineering college
Secunderabad , Telangana, India
rameshgarla497@gmail.com

Upendra Singh Aswal
Department of Computer Science & Engineering,
Graphic Era Deemed to be University,
Dehradun, Uttarakhand, India,
upendrasinghaswal@geu.ac.in

***Abstract*— The Internet of Things (IoT) system improves existing healthcare systems and their data. Specifically, the patient's sensitive data may be eavesdropped and linked to the identities of the sensors in transmission and thus revealing the patient's medical conditions. Therefore, in the such resource-impoverished environment, anonymous authentication for sensor nodes while considering their stringent resource constraints is a paramount security concern. In order to ensure security services and safeguard private customer data in the healthcare industry, this study proposes a new idea known as a secure anonymous authentication protocol with advanced encryption standards (SAAPAES). The suggested identification method offers a highly secure and effective identification scheme for the healthcare sector.**

Keywords*— *IoT, security, health-care sector, hash-key identification, SAAPAES algorithm

I. INTRODUCTION

In response to the need for numerous medical specialists internationally, which required connection between the professionals through video conferencing, the area of e-health has recently experienced considerable growth. However, it has become a distinctive aspect to keep a repository of the client that could be retrieved by a suitable doctor to understand the client's concern when it comes to a specialist knowing the medical experience of a client who is not knowledgeable on the technical expertise of his physical ailments [1]. IoT and cloud computing are cutting-edge, innovative techniques that, when combined to create adaptable, accessible, and effective patient healthcare services, enhance each other's potential. In contrast to typical networks, the integration is easier to establish and offers advantages notably improved information security during communication, instant access to documents, and energy efficiency. IoT-cloud-based e-Health technology can help healthcare services dramatically and encourage ongoing, methodical development. In IoT-cloud-based e-Health systems, interaction between clients, services, and servers is made possible by supporting IoT networks, and health records is saved in the cloud.

The IoT today uses IP-based connectivity to connect a wide range of systems, including sensors, to the Internet. IoT in the healthcare sector offers alternatives for wireless connectivity, early detection, and healthcare for institutionalised disabled people. For the IoT, individuals or things can be outfitted with sensors, actuators, RFID tags, and so on. Caretaker entry is made easier by certain tools and labels. For instance, IoT systems can read, recognise, locate, and manage RFID tags on clients' or clients' individual equipment (especially medical equipment) [15]. IoT makes it possible for a vast scope of intelligent applications and services to address difficulties that people or the medical industry confront [16]. To ensure an efficient medical system, this effectively integrates people, equipment, smart devices, and dynamic systems.

A cloud-based medical system assists in keeping the private information of clients and their medical issues in such circumstances. However, regrettably, the privacy and security of certain encrypted information have emerged as the primary worry [2]. Both cloud service suppliers and medical institutions should take necessary precautions to ensure the secure management of client records, particularly from being the victim of illegal offenders, in order to protect the privacy of patient records [3]. As a result, the cloud-based medical system must have strong security standards and assurances [4]. Companies must ensure that confidential health report information is maintained on the cloud in a more safe and encrypted manner so that they have no influence over the confidentiality of the data access systems used to send the information, or else it may pose a serious risk as network size and new network devices increase [5].

Government policies must be established to guarantee that cloud service suppliers follow all essential precautions to

protect the confidentiality of client data. There is a chance for effective data management with appropriate security if these standards are provided by cloud service suppliers. The client, whose data is stored in the cloud and who must have ownership over his medical information, is the first in line to express concern over privacy. The client should have special access rights so that they can only allow people with the right key inside.

In order to prevent people from entering the data in the cloud, the significance of certain encryption and decryption of information must be supplemented by a key [6]. A supplier selects the public and private keys for the encryption algorithm depending on the kind of encryption, and this supplier must identify themselves [7]. The permission technique typically entails providing the client's login credentials; the client is then connected or traced using their entry record or choices according to the data supplied to the cloud server during the permission [8].

Many IoT-based privacy-preserving identification methods have recently been suggested for safe data transmission and have been developed. The research showed the advantages of symmetric encryption, which processes data more quickly than asymmetric cryptography [9]. A homomorphic encryption method is employed to protect the files in the cloud from unauthorized users, and detailed research has explicitly emphasized that the approach is the adaptable and safe transmission of client personal medical data utilizing symmetric encryption [10]. The cloud-based system, which implements encryption, has found uses in many different fields.

However, when taking into account the study done by the scholars who were mentioned above, it becomes clear that no matter the type of cryptography used—symmetric (AES) or asymmetric (Elliptic Curve Cryptography, ECC), Rivest-Shamir-Adleman (RSA), etc.—none of these systems offer "total anonymity." However, the goal of our study is to enable clients to access medical care without disclosing their names, hence preventing eavesdropper tracing [11].

In this context, SAAPAES is suggested taking into account the privacy of the client records. In comparison to existing encryption/decryption methods, the SAAPAES-based medical system not only offers its clients the best level of security, but also lowers the encryption and decryption time on its terminals. For physicians to quickly find previous or present health history for emergency clients anywhere through networks, the SAAPAES also offers greater efficacy. Furthermore, we are confident that the symmetric cryptography we provide will facilitate quick encryption and decoding.

II. Literature Review

WBAN has been presented as a trailblazing important development for the future generation of ubiquitous medical systems as a result of the development of the IoT period and the rapid technological advances of wireless communications. Moreover, because of the flexible and adaptable characteristics of wireless sensor techniques, both sensor-controller and inter-sensor communications are susceptible to a number of possible threats, which seriously reduces the effectiveness of the WBAN and prevents ongoing development. In particular, the client's private information might be intercepted, connected to the names of the sensors in transmission, and used to determine the client's health. An important security challenge in such a resource-constrained scenario is unnamed identification for sensor nodes while taking into account their severe source limitations. In this research, we provide an unnamed authentication and key negotiation approach for WBAN applications that is both context-aware and compact [12]. The suggested system offers WBAN nodes selectable unnamed identification while accounting for dynamic context changes. The suggested method is safe from known attacks, according to a formal security study that uses the commonly used Real-Or-Random (ROR) model, Burrows-Abadi-Needham (BAN) logic, and an automated security standard evaluation method.

Technologies for the IoT include those for home automation, medical, transportation, etc. These products' major goal is to make users' lives better. Challenges to security and privacy as well as a dearth of appropriately tailored security measures, therefore, could greatly hinder their growth and use. To develop ways to secure IoT technologies and lessen or perhaps remove privacy risks, numerous studies have been carried out. Context-aware security, which permits taking into account pertinent relevant data while designing security protocols, is one of the methods that have been suggested. We shall perform a review of context-aware security solutions for IoT systems in smart cities in this article. These technologies do indeed have a significant effect on citizens' lives [13]. We will give a rigorous evaluation of each approach on the basis of safe context-aware control, protection, and confidentiality procedures. Next, we'll discuss the several study axes that could improve context-aware security in these apps.

IoT systems make it possible for efficient context-aware characteristics, which support the growth and advancement of ubiquitous computing. The IoT systems may recognise the customer's circumstance and modify their behaviour owing to these qualities. Additionally, they permit context-aware safety and confidentiality, which involves adjusting the installation of security and confidentiality measures to the customer's circumstances. The deployment of security and confidentiality measures is the main subject of study on context-aware security and privacy; nevertheless, safe and reliable context maintenance is not taken into account. We offer "SETUCOM," a novel safe and reliable context control system, in this study for context-aware security and confidentiality in the smart city. SETUCOM is the way the CASPaaS (Context-Aware Security and Privacy as a Service) paradigm implements the DTM (Device Trust Management) component. It controls credibility using AI methods like Bayesian networks and fuzzy logic, and protects context data transfer using a compact hybrid encryption solution tailored to IoT systems [13]. The suggested method is given a thorough description, and its key functions are assessed. The outcomes demonstrate the viability of SETUCOM for context-aware security and confidentiality in the smart city.

There is a lot of potential for an IoT-based e-health service. The adoption of ubiquitous bio-medical sensor devices, cloud computing, big data analysis, and smart mobile medical devices has significantly altered the business model and usage behaviour of IoT-based e-health services. Security and confidentiality problems are associated with the Internet of Things-based e-health services' rapid growth. We suggest

a brand-new security system for an e-health service in this research. In order to protect the acquisition of medical records, this technique enables mutual authentication between the local base station and hospital cloud server. The validity of identification transactions is checked by our system using the crypto hash function [14]. A session key agreement is reached among each local base station and the hospital cloud server, and it also offers mutual identification with anonymity. We undertake security and effectiveness framework to examine our plan. The outcomes demonstrate the security, portability, and threat resistance of our method.

To protect e-health systems in the context of the IoT, key distribution is necessary. IoT resource limitations prevent these systems from using the current key management methods, nevertheless. We suggest a brand-new, compact key management method in this work. A very resource-limited node and a remote entity can build a safe end-to-end communication channel using this approach, which is based on cooperation. The limited node can send recorded data while maintaining privacy and identification owing to the secure channel. We suggest delegating resource-intensive cryptographic techniques to third parties in order to accomplish this objective. The confined node thus receives support from strong entities. We do a rigorous evaluation considering security features to evaluate our approach [17]. In order to emphasize energy efficiency, we also examine the expenses associated with communication and calculation. The findings demonstrate that our technique offers a sizable energy yield while maintaining its security attributes.

III. RESEARCH METHODOLOGY

The framework of the suggested method, the transit of medical data, accounting, identification, and enrolment are all covered in this part. The suggested solution offers an opportunity where a client's private medical records are kept in the cloud and accessible by any authorised doctor to learn about the client's medical history before they meet. Each person's medical history is handled by this, and all accredited hospitals have permission to view or modify the information for use in the later by any other qualified physician [18]. The organization must be enrolled and may have obtained a licence that is stated as a "unique database accessing code" before it may access the database. An identifying code will be produced when the client information is being stored in the database. Every time patients receive treatment; their health data will be entered into the database using their identification code without their consent or revealing any personal information.

The suggested framework and process model for SAAPAES are shown in Fig. 1. When the client's information is first gathered from the WBAN sensor nodes, it is kept in a PDA. Due to this, the hash key method will be used to enroll the physicians and clients. Only clinicians who have the client authentication code, or ID, can view the client's basic data profile. By providing them with the cloud data that has been uploaded, clients can examine numerous physicians [19]. The medical files often include information on numerous disorders. Two identification keys are a vital component of our suggested approach for protecting healthcare data.

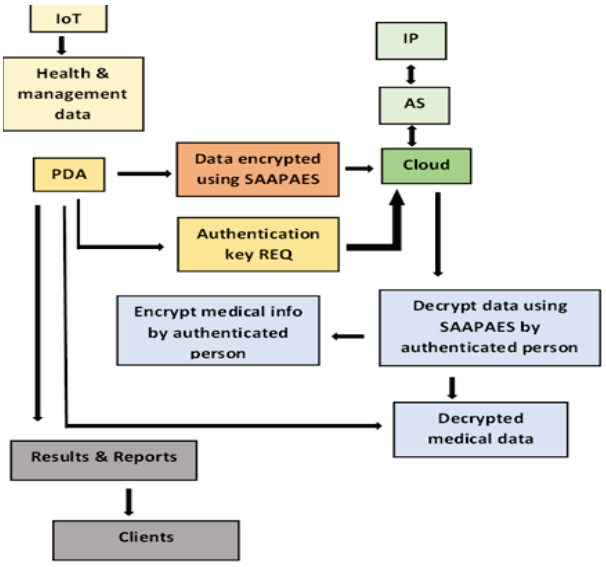

Fig. 1. Proposed SAAPAES Architecture

It should be emphasised that anyone who wishes to examine their records will only be able to do so by granting access over their recorded private details due to security concerns. This will assist the client in making sure that their private details are neither inflated or incorrectly understood [20]. However, on the same note, any modifications can only be made by a physician with the necessary technological expertise in medical services, prohibiting laypeople from altering any information's technical significance.

IV. RESULTS AND DISCUSSION

The aforementioned analytically proven research was deployed in the Cooja toolbox, and as illustrated in figure 2, homomorphic encryption is used to establish security. The security was applied to the data once it was retrieved from the SQL database.

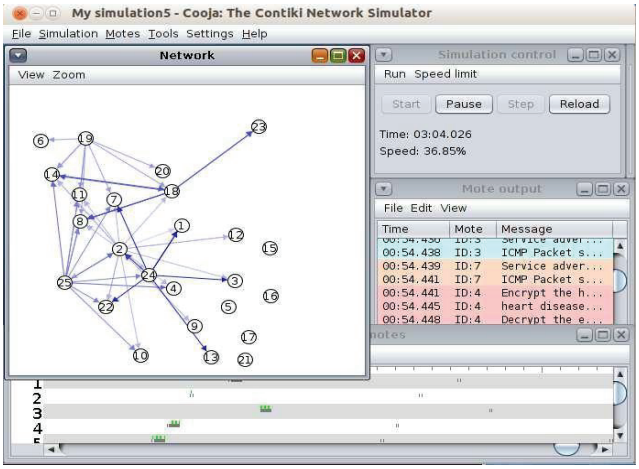

Fig. 2. IoT simulation result

A. Encrypting the data using SAAPAES

The technique of authenticating a customer's right to access a specific platform is known as authorization. To upload a file to the cloud, a distinct file ID is formed. This ID

can be used by authorised users to retrieve and modify their uploaded data. These values are encrypted using the SAAPAES encryption technique after a healthcare file has been uploaded. For encrypting plain text, a key size of 128 bits is used. Fig. 3 demonstrates how client data is protected at the user end and is kept encrypted at the IoT server.

Original Data	Encrypted Data
2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy	x »(æ!* ¥ÉLöt¿#"ÊT^ Øñv¤éó ~¢zJÔ ¯Ø ¸ã*T² ôi»> 9ëÂ8j ÎV¿NôË]|è & +:&øí

Fig. 3. Encrypted data

B. *Decrypting the data using SAAPAES*

The cloud-based encryption messages will be downloaded and then decoded to reveal the original plaintext. Physicians and other clients that require the healthcare data have access to a private key that is used to perform the decryption. The SAAPAES technique, which is also used to decrypt text files, generates the key. Fig. 4 displays decrypted user data that was securely saved on an IoT server using a hash identification key.

Original Information	Encrypted Information	Decrypted Information
2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy	x »(æ!* ¥ÉLöt¿#"ÊT^ Øñv¤éó ~¢zJÔ ¯Ø ¸ã*T² ôi»> 9ëÂ8j ÎV¿NôË]|è & +:&øí	2020 Dr.Rajesh Rakesh 55 boduppal malignant tumour 19-02-2020 brain tumor biopsy

Fig. 4. Decrypted data

C. *Performance evaluation*

Place SAAPAES is an effective way because, according to simulations performed with the Cooja toolbox, it uses less energy than other available algorithms. Here, SAAPAES with a 128-bit key is used for both encryption and decryption of the data. In aspects of calculation time, network lifetime, adaptability, congestion, security, and encryption and decryption times, the simulation outcomes enabled us to contrast SAAPAES with DES, BLOWFISH, and AES algorithms. The calculation time is the amount of time needed in the cloud system to compute and validate the keys. The 117ms computing time of the SAAPAES method is achieved. The proposed method's time is found to be shorter than the currently used DES, BLOWFISH, and AES, which have times of 216 ms, 178 ms, and 142.5 ms, respectively. Fig. 5 shows a contrast between the suggested SAAPAES and the current algorithm.

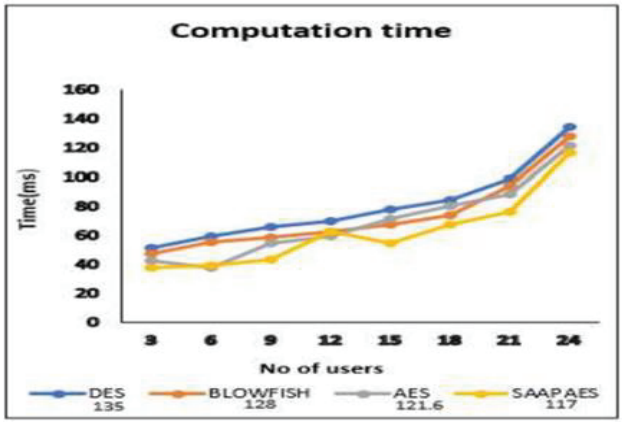

Fig. 5. Computation time

Another crucial performance indicator in the suggested security model is the network lifespan (NL). The total amount of active time that the node can maintain throughout an efficient data transfer is known as the NL. The network lifespan of the suggested SAAPAES approach is around 249.64 seconds, which is superior than the network lifetimes of the current techniques, which are 120, 125, and 227.64 seconds. Fig. 6 compares the performance of the current method and SAAPAES over the network lifetime.

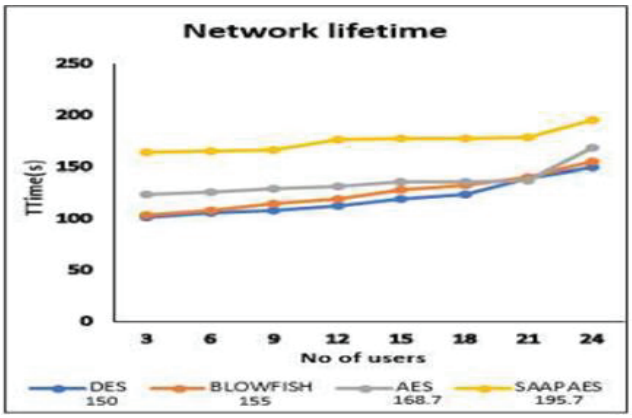

Fig. 6. Network lifetime

The amount of delay experienced during data transmission in the cloud is known as latency. The suggested SAAPAES strategy achieved a latency of 0.382ms compared to the previous methods' latency of around 0.431ms, 0.76ms, and 0.1ms. Fig. 7 compares the latency effectiveness of SAAPAES with that of existing methods.

The capability of the cloud to manage the materials that are maintained there is measured by its adaptability. The adaptability of the suggested SAAPAES is 0.896, greater than that of the previous techniques, whose scalabilities are 0.59 ms, 0.89 ms, and 0.731 ms. Fig. 8. compares the adaptability of the suggested SAAPAES and the current approach.

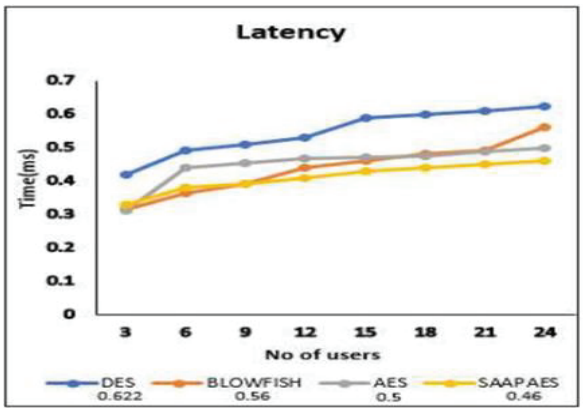

Fig. 7. Latency

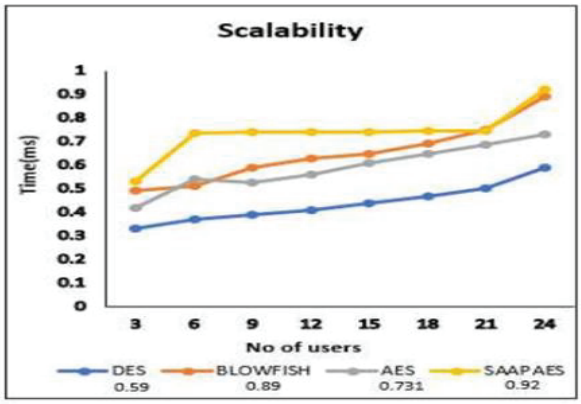

Fig. 8. Scalability

The most crucial components of any security technique are security, encryption, and decryption time. Fig. 9. shows that SAAPAES's encryption and decryption times are 40 ms and 69 ms, respectively, which is faster than the times for the current approaches of 48 ms and 90 ms, 87 ms and 76 ms, and 41 ms and 80 ms.

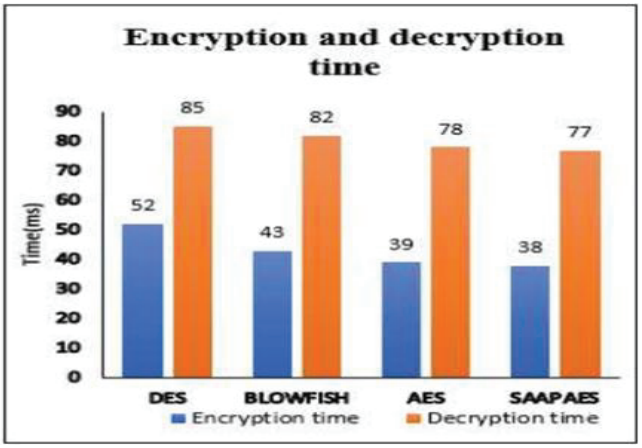

Fig. 9. Encryption ***and decryption time***

Fig. 10 compares the suggested SAAPAES algorithm's security level, which is approximately 89%, to that of the existing techniques, which have security levels of 76%, 75%, and 86%.

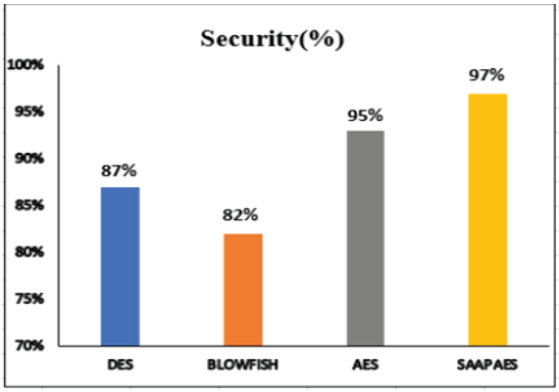

Fig. 10. Security

V. CONCLUSION

In this work, the implementation of Context Aware in order to aid in the assistance of end users within the framework of e-Health scenarios has been described. Healthcare sectors need innovative and affordable methods to assist medical organisations in identifying additional successful tactics to handle the volume of client records [21]. In addition to metropolitan areas, this IoT-based medical system would undoubtedly assist the local population with a cost-effective strategy, saving them from having to drive long distances to see a doctor. But for such a system to succeed, users' faith must be earned, and this trust is closely correlated with the level of protection or confidentiality offered to their information. This has always driven academics to pursue novel cryptography methods that can excite users. In such a scenario, this work showed message encryption and user/person identification using a unique identification number without disclosing any other information about them. Thus, we were able to create an encryption method for unnamed identification and significantly enhance its effectiveness [22]. According to simulations, the 128-bit SAAPAES encryption strategy has improved and reinforced record security to the highest level of secrecy with little energy usage.

Each author gave a substantial contribution in the acquisition, analysis and data interpretation. Each author had a part in preparing the article for drafting and revising it critically for important intellectual content. Each author gave final approval of the version to be published and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

VI. FUTURE SCOPE

We will provide context-aware security techniques in the upcoming, in which identification and authorisation policies are dynamically and adaptively chosen based on context changes. In order to resolve the tension between security and energy use, we shall actually deal with the issue of adaptive security in WBAN. The solutions proposed to ensure privacy-preserving in a context-adaptive manner in the projects discussed above only propose a mechanism with several limitations, and most of them are still at the proposal stage.

REFERENCES

[1] Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.

[2] Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., & Vasilakos, A. V. (2018). An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Computers & Electrical Engineering, 69, 534-554.

[3] Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. IEEE Wireless communications, 17(1), 51-58.

[4] Zanjal, S. V., & Talmale, G. R. (2016). Medicine reminder and monitoring system for secure health using IOT. Procedia Computer Science, 78, 471-476.

[5] Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 78, 659-676.

[6] Yang, Y., Zheng, X., & Tang, C. (2017). Lightweight distributed secure data management system for health internet of things. Journal of Network and Computer Applications, 89, 26-37.

[7] Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2019). Reducing the required time and power for data encryption and decryption using K-NN machine learning. IETE Journal of Research, 65(2), 227-235.

[8] Tang, J., Liu, A., Zhao, M., & Wang, T. (2018). An aggregate signature based trust routing for data gathering in sensor networks. Security and Communication Networks, 2018.

[9] Song, C., Lin, X., Shen, X., & Luo, H. (2013, October). Kernel regression based encrypted images compression for e-healthcare systems. In 2013 International Conference on Wireless Communications and Signal Processing (pp. 1-6). IEEE.

[10] Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2013, October). Secure medical architecture on the cloud using wireless sensor networks for emergency management. In 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 248-252). IEEE.

[11] Sowjanya, K., Disrupt, M. & Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int. J. Inf. Secure. 19, 129– 146 (2020).

[12] Arfaoui, A., Kribeche, A., & Senouci, S. M. (2019). Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. Computer Networks, 159, 23-36.

[13] Sylla, T., Chalouf, M. A., Krief, F., & Samaké, K. (2021). Context-aware security in the internet of things: a survey. International journal of autonomous and adaptive communications systems, 14(3), 231-263.

[14] Hussien, Z. A., Jin, H., Abduljabbar, Z. A., Hussain, M. A., Yassin, A. A., Abbdal, S. H., ... & Zou, D. (2016, August). Secure and efficient e-health scheme based on the Internet of Things. In 2016 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC) (pp. 1-6). IEEE.

[15] Tesoriero, R., Gallud, J. A., Lozano, M. D., & Penichet, V. M. (2009). Tracking autonomous entities using RFID technology. IEEE Transactions on Consumer Electronics, 55(2), 650-655.

[16] Medaglia, C. M., & Serbanati, A. (2010). An overview of privacy and security issues in the internet of things. The internet of things, 389-395.

[17] Abdmeziem, M. R., & Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. Computers & Electrical Engineering, 44, 184-197.

[18] V. Panwar, D.K. Sharma, K.V.P. Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations and Optimization of Surface Roughness in Turning of EN 36 Alloy Steel Using Response Surface Methodology and Genetic Algorithm" Materials Today:

[19] A. Jain, A. K. Pandey, (2019), "Modelling and Optimizing of Different Quality Characteristics in Electrical Discharge Drilling of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191

[20] A. Jain, A.K. Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics in Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684

[21] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations in Electrical Discharge Drilling of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261

[22] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Fibre Matrix Composite through Electric Discharge Machining: A short review" Material Today Proceedings.