Advanced Machine Learning in Secure Authentication for Users in Healthcare Application

Sumit Kushwaha

Department of Computer Applications, University Institute of Computing, Chandigarh University, Mohali, India

Abstract

Networking and data communications technologies have evolved more rapidly thanks to sustainable computing. The idea of developing intelligent health systems is currently taking shape as the Sustainable Healthcare Systems. The study of security for Sustainable Healthcare Systems-based application systems, including such e-healthcare systems, industry automation systems, tactical surveillance systems, and so on, has recently made considerable achievements in the academic world. Chaotic Map assisted SHA-3 algorithm is discovered as a crucial security-control method to the design of Smart Environments. The S-USI assigns a unary-token to the authorised users so they can access the various services offered by a service provider across an IP-enabled distributed system in order to guarantee fidelity. There are many authenticating methods available for cloud-based decentralized systems. The majority of the techniques are still susceptible to security risks like replay attacks, powerful intrusion attempts, user request, and authentication protocols. In order to provide security and privacy, the intelligent healthcare industry described in this study help of sensors and sensor-tag technology. A strong secured based mechanism and well-formed cohabitation protocols proof for ubiquitous cloud services are suggested in order to bolster the authentication process. The significance of the proposed measures is demonstrated to demonstrate the security effectiveness of the suggested method using a formal security analysis. The comparison has been done from the formal verification show that the presented method uses less overhead processing, making it more appropriate for telemedicine hospital information systems.

Keywords

Secure Authentication, Users Records, SHA-3 Algorithm, Sustainable Healthcare Systems, SDG

1. Introduction

The ultimate goal of such an exploration is to address the flaws of the existing security systems [1,2]. International institutions as well as individual users have attracted to the new and fast growth of cloud computing due to the nature of provisioning which has adopted the concept of pay-as-you-go and has thus become highly attractive to organisations and consumers [3,4]. This increase is reflected not only in the maturing infrastructure and variety of services provided by cloud computing, but a significant rise in the number of organizations moving their operations to cloud-based environment in attempt to find scalability, flexibility in their operations and their reduced cost [5,6].

The global trend towards cloud computing is picking up pace, so the inevitable problem is management and security of large volumes of data in cloud-based environments. At the moment, preliminary statistics show that as of the year 2020, the future of up to 83% of organizational task loads have been projected to have shifted to the cloud and thus the more reliant on cloud services [7-9]. This rapid adaptation is transforming cloud computing into an on demand environment where consumer demand instant access to data and services with out interruption or latency [10]. Nonetheless, this fast development has also come up with a number of essential concerns the first most involving security, data integrity, scalability and privacy, as in Figure 1 [11,12].

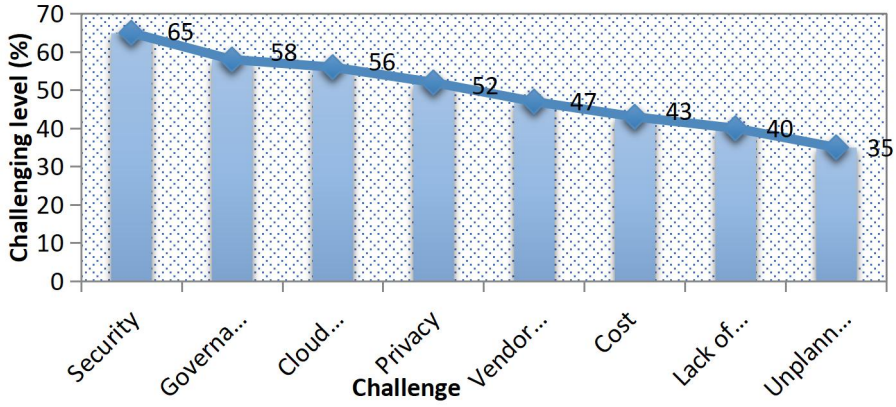

Figure 1. challenges in cloud computing

Cloud computing has emerged as an essential part in the information technology systems of organizations [15,16]. However, its skyrocketing embrace has increased the imperativeness of meeting challenges arising because of performance. According to recent scholarly surveys, over 60 percent of the estimated disquiets about cloud revolve around the matters of security and privacy challenges [14]. The findings support the idea that there is a need to come up with resilient security strategies that would help secure sensitive data in the cloud platforms that have now become the backbones of the IT infrastructures.

One of the most representative examples is the control of electronic health information. Healthcare industry, one of the most confidential of all types of information, has been resorting to the adoption of cloud computing more to improve the smoothness of operations and service provision [18]. Electronic health (eHealth) systems are a revolutionizing move towards the goal of providing better, efficient and accessible healthcare. An eHealth platform has to be flexible, stable and sustainable to meet such expectations. But the Personally Controlled Electronic Health Record (PCEHR) technologies in wide application assert an incomplete control over the data of the patients, thus creating danger of allowing the unauthorized hands (medical practitioners or the operators of repositories) of the information get access to some important information. Such intervention raises a very serious concern that needs to be looked at more keenly when it comes to data integrity and data security in cloud settings [19,20].

The issues of privacy when storing and sharing electronic health records (EHR) in cloud settings are of a heightened nature. The existing technologies claiming to facilitate safe access to EHR do not guarantee full confidence due to ineffective authentication process which can lead to data exposure and unauthorized access to them [21,22]. Owing to the highly sensitive nature of health-related information, only qualified medical specialists and healthcare administrators should access the same. This is why it is important to implement stricter procedures of authentication [23].

The literature shows that the current authentication systems deployed in cloud-based eHealth systems should be improved. The current paper brings a hybrid access control model that would overcome the given weaknesses [24]. Contributing to the protection of the health data at rest and in transit, the model introduces layered security barriers due to integrating various communication channels, such as biometric systems, token-based solutions, and encryption techniques [25].

Other important considerations are scalability and adaptability. The importance and scale of the health data have grown, and cloud elements have advanced, thus altering the scale and specifics of authentication and access control systems, although they are necessary to guarantee protection throughout the data life cycle [26]. The flexible nature of the hybrid solution will be enough to ensure that such fluctuations are taken into account, and still, patient privacy is not in danger as maturity is achieved across cloud environments [27].

Looking at overview of results, it is observed that stronger and more secure authentication tools are necessary in eHealth sector, particularly, in cloud computing environment [28]. The sensitivity in data that is health-related and the speed at which cloud solutions are reported to be advanced requires proper protection protocols to prevent malicious activities [29]. The described here hybrid access control model is more versatile and complete, as such, will further promote the privacy and security of eHealth information. When properly executed, then it would lay the brick of more reliable and secure cloud-based eHealth systems and support both patient privacy in a fast-changing digital world [30,31].

2. Literature Review

The following work introduces a new-fangled three-factor authentication (3FA) scheme that can be used to protect Internet of Things (IoT) Wireless Sensor Networks (WSNs). The scheme is based on a mobile authentication infrastructure that depends on the extraction of the biometric characteristics of the users. Its main target is to increase the safety and effectiveness of smartphone applications, IoT, which are being implemented in a growing list of applications. Combined with biometrics, intelligent gadgets, and usual password systems, the procedure of authentication becomes both safe and comfortable at once. The protocol given in the article is based on the cryptographic tools that are well known, that is, hash functions and XOR (operations). It has four basic elements of user access protection [32,33]:

a) Three Factor Authentication (3FA). This aspect is a collision of three elements:

- What the user possesses; a smart device;
- Something that the user possesses-biometric features, namely his fingerprints.
- Something that the user knows- the password.

b) Shared Session Key. After the authentication of the user, this key is used to encrypt subsequent data in the session, thus increasing protection to the data.
c) Mutual Authentication. Each must authenticate the other, the user and the IoT system, thus preventing the man in between (MITM) attack scenario where an attacker intercepts messages between two parties.

d) Key Freshness. The session keys are refreshed regularly and therefore the chances of replay attacks where an attacker reuses past messages to personate a valid user are reduced.

In order to consider the authentication protocol proposed holistically, the researchers involve the use of several formal methodologies where the Burrows-Abadi-Needham (BAN) logic stands out. There is analysis logic and a precise method of proving the correctness of security protocols named BAN logic. In addition, the simulation platform, the Automatic Validation of Internet Security Protocols and Applications (AVISPA) is used, to have a model of the authentication scheme and explore its security properties in a variety of operational conditions. Complementary informal security analysis promotes the protocol by demonstrating the manner it translates several possible vulnerabilities [34,35].

The paper proves that the suggested scheme can outweigh by far the current robust authentication schemes in security, convenience, efficiency of communication and computational overhead. The protocol enhances the security environment of the Internet of Things (IoT)-based application, particularly in Wireless Sensor Networks (WSN), largely due to the three-factor schematic making use of biometrics, smart devices, and traditional passwords [36,37].

Wireless Body Area Networks (WBANs) are one of the rapidly developing segments of the IoT, which have won popularity in therapeutic applications. The wearable sensors used on WBANs enable a continuous data collection and sending of physiological or behavioral data which forms the basis of the next generation of the medical systems. Such networks can carry the real-time reporting of measurement including heart rate, blood pressure, temperature, and other vital signs [38,39].

Body-worn wireless sensor networks (WBANs) are a special type of a wireless network that is likely to transform a variety of fields, particularly the health sector. However, implementation of the same keeps facing non-negotiable problems, top among them concerning privacy and security. Due to the fact that WBANs communicate with the help of unencrypted wireless protocols, they are quite vulnerable to eavesdropping, data modification, and unauthorized access notifications. Such weaknesses present strong hurdles, particularly when in a healthcare setting, where data integrity has strict standards that need powerful defensive measures to be met on confidential data [40,41].

Another hindrance is that most implanted sensors are of limited capacity. Such devices are usually small, battery powered, and have limited resources, but are required to transmit, store and crunch data to within tightly specified power and memory limits. Any secure-communication protocol used in such a setting has to be effective without prohibitive computing costs [42].

Employing smartphones as intermediates creates an attractive channel in curbing the security risks of widespread body-area networks (WBANs) [43]. On the basis of the high computation capabilities and storage facilities, as well as the ubiquity of these mobile devices, WBANs can share the computational and storage burden and maintain their end-to-end security through air-borne transmission of data. With the arrival of the fifth-generation (5G) of network infrastructure, the role of smartphones in the safe gathering and sending WBAN data will increase further [44,45].

In the proposed paper, the standard WBAN architecture suggests replacing the traditional personal controller (PC) with a smartphone application program. Such a replacement will allow processing sensor information more efficiently and integrating it without any issues with cloud-based healthcare systems. Additionally, smartphone acts as the mediator between limited sensors and distant clouds or devices, hence providing protection of data confidentiality and integrity involving patient information [46].

Biometric authentication, by charging, allows passable authentication of individuals on an electrocardiogram (ECG) recording. ECG has high biometric discriminability that could be easily detected using wearable sensors to conduct effective personal identification. The features obtained with the help of ECG when fed into a three-factor authentication system provide extra protection against impersonation [47,48].

An important part of the protocol process is the group key management: in case of a process related to a single user multiple co-located sensors can be deployed and thus secure communication among the devices is required. The phone part of a smartphone choreographs the release of the session keys to all the sensors approved to participate in responding to the query, and the data transmitted at the time secures privacy [49].

The resilience of the system is additionally optimized by dynamic key updating. Revision of the encryption keys according to a regular schedule can thwart replay attacks, as well as long run compromise of older keys. The process does not require any considerable alteration of already deployed sensors and has assured scalability and efficiency in computation. To conclude, the provided scheme combines biometric verification based on ECG with group key establishment and key refreshment, thus ingraining sensitive WBAN data at the cost of limited computational and comminative overheads. The efficiency and security of the protocol are increased by high processing capabilities and off-body storage of the smartphone. The study highlights the need of performance-optimised, scalable and privacy-friendly authentication systems to the growing Internet of Things (IoT) environment [50].

3. Proposed Work

In order to enforce a secure authentication protocol, a host system and a sensor/peripheral module must be connected. A

1-Wire SHA-256 safe authenticator and a SHA-256 coprocessor with a 1-Wire master function make up the system shown in Figure 2. Working more than a single pin of the 1-Wire interface between both the hosts and peripherals improves design, lowers costs, and decreases connection complexities.

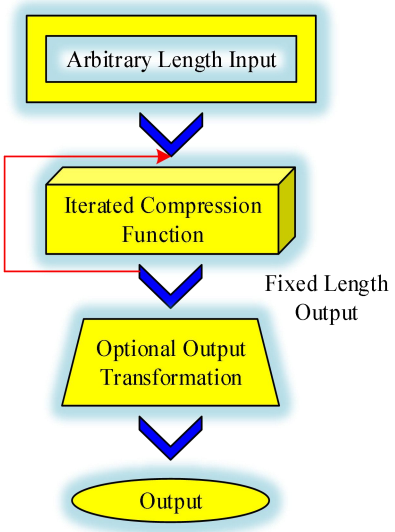

Figure 2. Formation of hash function

However, certain functions describe the hashing algorithm is strong as follows:

(1)

$$h(x) = H \tag{1}$$

(2) Weak Collision Resistance

$$h(x) = h(y) \tag{2}$$

(3) Strong Collision Resistance

$$h(y) = h(x) \tag{3}$$

The most significant properties of using secure hash function can be follows:

h_i is considered as an input for Md_i at any size of the packet

It is most simple to calculate the secure hashes.

It comprised of collision free property and thus it does not produce any unique outcome for two or more inputs.

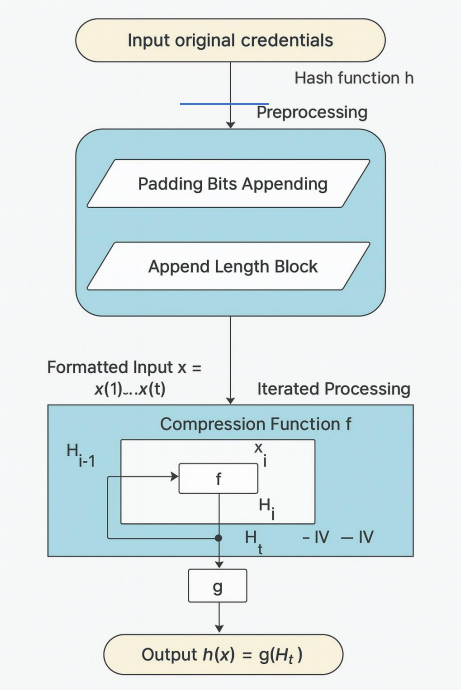

Figure 3. Formation of hash code from credentials

In order to compute a hash function, a mobile node selects the random variable $r \in (0,1)^{\alpha}$ and then computes list of values by r (H_0, H_1, H_2, H_3, ... H_n) where $H_0 = r$ and $H_i = h(H_{i-1})$ for $0 < i \leq n$. SHA family (SHA0, SHA1, SHA2, and SHA3) is created by NIST standard. Each hashing algorithm can be characterized using output size, block size of bits, word size (bits) and multiple hashing functions, as in Figure 3. This will reflect the changing in message integrity with high probability rate. If compare SHA3 with SHA2, SHA3 provides high security and SHA-2 requires 64 cycles, but SHA3 needs 24-cycles of operation. When number of cycles increase, SHA3 increases the hashing speed than SHA2. SHA3 is based on the Keccak Sponge Construction. A main feature of SHA3 is that is highly flexible and robust against traditional hash functions. Table 1 shows the SHA properties and Figure 4 shows comparison of hashing algorithms.

Table 1. SHA properties

SHA type	Word Size (Bits)	Message Size (Bits)	Block Size (Bits)	Message Digest Size (Bits)
SHA-1	32	Less than 264	512	160
SHA-224	32	Less than 264	512	224
SHA-384	64	Less than 2128	1024	384
SHA-512	64	Less than 2128	1024	512
SHA3-224/512	64	Less than 2128	1024	224
SHA3-256/512	64	Less than 2128	1024	256

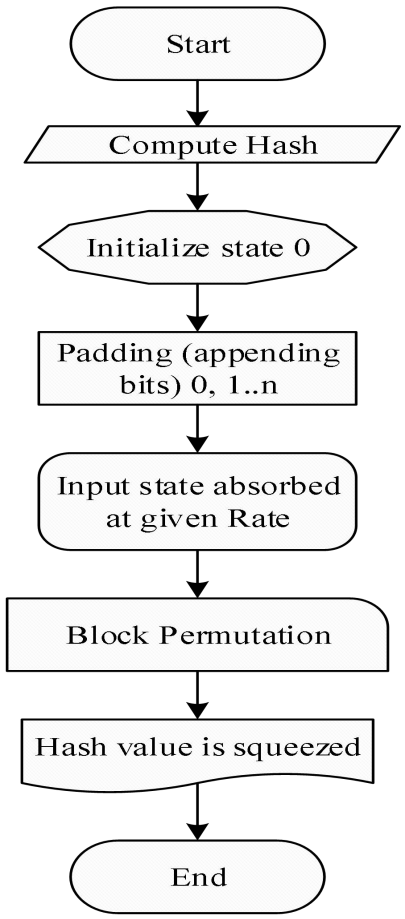

Figure 4. Flow diagram for SHA-3

It considers variable size input and results variable length output and the parameters of SHA-3 are Rate r and Capacity c. A unit of these two parameters is bits. In addition, rate is the hashing speed and capacity means the permutation security level. The permutation of b is $r + c$. A Keccak Sponge Construction is represented as,

$$R = (i) \oplus (X) \oplus (\pi) \oplus (\rho) \oplus (\theta) \quad (4)$$

where, i is the iota module which breaks up any symmetry that causes due to other modules. It estimates the array elements for a round of constant. Its nearly takes 24 rounds chooses using Keccak Sponge Construction. When without iota module, all rounds of mapping will be symmetric. X is the Chi module that adds nonlinear function to the permutation round. It combines the row elements using 3 bitwise operators include && (and), ! (not) and $\oplus$ (ex-or). In the final analysis, it stores the result in a state array, pi (π) is the permutes of 64-bit elements where permutation will work with a fixed pattern assignment, ρ is the rho module which rotates the 64-bit elements by triangular numbers 0, 1, 3, 6, 10, and 15, and theta (θ) renders the internal state into 5 $\times$ 5 array of 64bits. It calculates each column elements and integrates them with an XOR operator and then it results parity for each state bits. Then number of rounds computed using $12 + 2l$ and keccak $f(r+c)$ is calculated. For instance, r is the 1024bits and c is the 576bits. In the final analysis, Keccak f is the 1600 for 24 rounds. It utilizes byte ordering and bit numbering. A process for SHA3-256 can be described as follows:

- Consider an input as credentials of mobile user and add on the delimiter.
- It uses the Keccak Sponge Construction where message blocks are XOR into a subset of the state. Then execute the change to obtain the whole file.
- Next execute padding i.e., appending bits, absorb the input into the state i.e., for each piece XOR it into the state and then block permutation is applied.
- The hash values for user credentials are computed at same rate as input file. The flowchart for SHA-3 (512bits) is depicted.

Algorithm 1 SHA-512 Algorithm

1: Begin
2: Initialize the number of users
3: For all the users
4: Initialize registration
5: Get the input parameters for registration
6: Generate the message for each user parameters by fusion
7: Do padding bits to the original message
8: Append length
9: Initialize the chaining variables
10: Assign the all-chain variables into new variables
11: Process all the number of blocks
12: Splits the input message into 512 bits of blocks (16 sub-blocks and each with 32 bits)
13: SHA-512 performed with 4 rounds and each consists of 20 steps
14: Consider three inputs for each round (512-bit block, register for chain and constant variable)
15: For rounds 1 to 4
Round 1 is performed between 1 to 19
Round 2 is performed between 20 to 39
Round 3 is performed between 40 to 59
Round 4 is performed between 60 to 79
16: Perform SHA-512 for 80 rounds
17: For each iteration, logic, register, circular left shift, and additive operations
18: Generate the final hash by fusing all blocks
19: End registration and then perform authentication
20: Collect input parameters and compute hash by performing step (7) to (18)
21: Compare Hash (i) and Hash (j)
22: if matched, then return authentication is successful
23: Else terminate the authentication
24: End if
25: End for
26: End

4. Experimental Results & Discussion

The experiment test is conducted to evaluate how well our verification method worked. Test results, as in Figure 5, demonstrate that the proposed method can complete authentications with tolerable delays. Because the suggested hashing methods are more sophisticated than previous systems and it is impossible to determine the precise plaintext password because it is hidden among a huge number of false passwords, they are resistant to password guessing attempts. Additionally, our system is protected against attacks using stolen verifiers, because even if the attacker has the password, they still need the delimiters since they're not recorded on the server. In the proposed, we assume that the

networking and servers employ safe cryptographic techniques like SSL and cutting-edge validation tools to fend off Man-in-the-Middle attacks, Replay attacks, and Dos attacks.

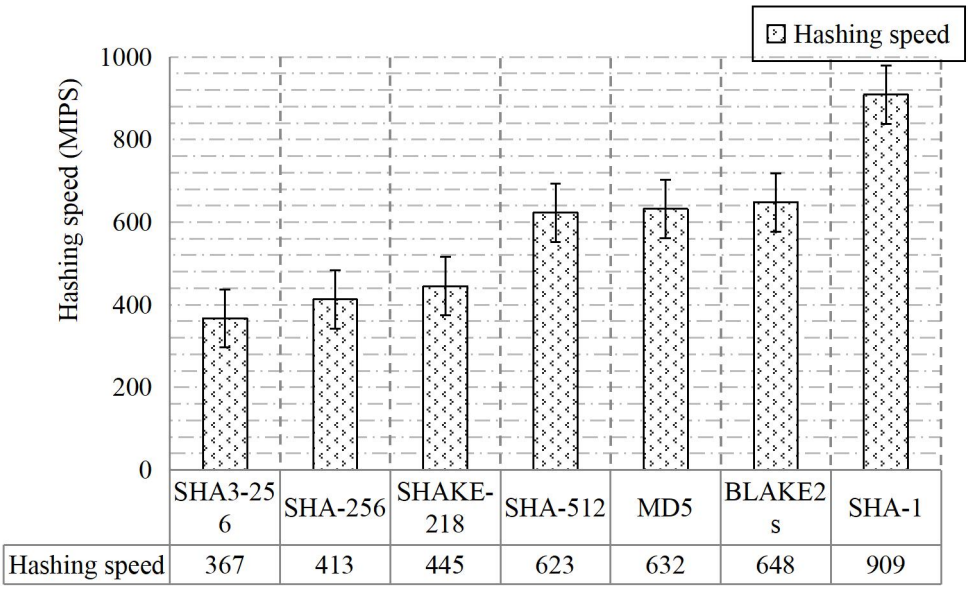

Figure5. Comparison of hashing algorithms

On the other hand, submitting an user name and password just at time of access is typically accepted as an option. Even simplified methods might be favoured as ICT use increases (e.g., the use of fingerprints for smartphones). However, such easy and passive processes can then be used to prove intention. Especially when it comes to the widespread the use medical and health data, they may significantly increase the chance of individuals agreeing without giving the decison significance and ramifications due thought. In those other words, it is impossible to ensure the integrity of professional researchers and practitioners. As a result, it's critical to perform appropriate actions, including submitting a login and password as a means of security even during login. It is unclear whether a signature in a consent form regarding medical care and study may be satisfactorily replaced by this type of authentication. Views have changed over time and in different locations, but now at least for the time being, a straightforward action like a click shouldn't be taken for granted.

5. Conclusion & Future Work

In the research, a number of passwords, biometrics, and smartcard reader remote user authentication techniques have been presented. The majority of the systems put out in the research, unfortunately, are either computationally costly or vulnerable to a number of well-known attacks. We seek to introduce a novel, strong, and efficient password-based remote user authentication technique in this study. Our system is effective because it only employs a one-way hash function and bitwise XOR procedures that are efficient. We demonstrate that our system is secure against potential attack patterns using rigorous informal and formal security research. Additionally, appropriately and accurately handles the password change process without ever accessing a remote server. Our system also outperforms competing techniques in terms of communications, computational overhead expenses, privacy, and features accessibility.

References

[1] K Rai, A., Singh, S., & Kushwaha, S. (2024). Optimized handwritten digit recognition: A convolutional neural network approach. 2024 International Conference on Communication, Control, and Intelligent Systems (CCIS), 1-5. Mathura, India.

[2] Rai, A., Singh, S., & Kushwaha, S. (2024). Hybrid watermarking techniques in medical imaging: A comprehensive analysis and performance evaluation. 2024 International Conference on Communication, Control, and Intelligent Systems (CCIS), 1-5. Mathura, India.

[3] Sharma, G., & Kushwaha, S. (2024). A comprehensive review of multi-layer convolutional sparse coding in semantic segmentation. 2024 9th International Conference on Communication and Electronics Systems (ICCES), 2050-2054.

[4] Kushwaha, S., Kondaveeti, S., Vasanthi, S. M., W, T. M., Rani, D. L., & Megala, J. (2024). Graph-informed neural networks with green anaconda optimization algorithm based on automated classification of condition of mental health using alpha band EEG signal. 2024 4th International Conference on Sustainable Expert Systems (ICSES), 44–50.

[5] Kushwaha, S., & Rai, A. (2024). Mobile cloud computing: The future of cloud. 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0, 1-6.

[6] Kushwaha, S., Sathish, P., Thankam, T., Rajkumar, K., Kumar, M. D., & Gadde, S. S. (2024). Segmentation of breast cancer from mammogram images using fuzzy clustering approach. In Proceedings of the 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-6). Chennai, India.

[7] Singh, C., V, S. R., Vyas, N. K., Gupta, M., Kushwaha, S., & Prasanna, N. M. S. (2024). Sending query data to mobile sinks at high speed in wireless sensor networks. In Proceedings of the 2024 Ninth International Conference on Science Technology

Engineering and Mathematics (ICONSTEM) (pp. 1-5). Chennai, India.
[8] Kushwaha, S., Amuthachenthiru, K., K, G., Narasimharao, J., M, D. K., & Gadde, S. S. (2024). Development of advanced noise filtering techniques for medical image enhancement. In Proceedings of the 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 906-912). Tirunelveli, India. https://doi.org/10.1109/ICICV62344.2024.00149.
[9] Kumar, V., & Kushwaha, S. (2024). Optimized hybrid metaheuristic model for MapReduce task scheduling applications – A novel framework. In Proceedings of the IEEE 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2024) (pp. 1-7). Tirunelveli, India.
[10] Kushwaha, S. (2023). An effective adaptive fuzzy filter for SAR image noise reduction. In Proceedings of the IEEE Global Conference on Information Technologies and Communications (GCITC) hosted by REVA University (pp. 1-5). India.
[11] Kushwaha, S., Boga, J., Rao, B. S. S., Taqui, S. N., Vidhya, R. G., & Surendiran, J. (2023). Machine learning method for the diagnosis of retinal diseases using convolutional neural network. In Proceedings of the IEEE 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (pp. 1-6). Chennai, India.
[12] Kushwaha, S., V, A., Kumar, B. S., Singh, N., Prabagar, S., & Supriya, B. Y. (2023). Efficient software vulnerability detection with minimal data size in 5G-IoT. In Proceedings of the IEEE 2023 International Conference on Emerging Research in Computational Science (ICERCS) (pp. 1-6). Coimbatore, India.
[13] Kumar, V., & Kushwaha, S. (2023). Comparative study of map reduce task scheduling optimization techniques. In Proceedings of the IEEE 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT) (pp. 1-7). Bengaluru, India.
[14] Kousar, H., Fatima, S., Ahmed, S. I., Sajithra, S., Kushwaha, S., & Balaji, N. A. (2023). AI-based security for Internet of Transportation Systems. 2023 4th International Conference on Smart Electronics and Communication (ICOSEC), 701–708, India.
[15] Singh, C., Jayakumar, S., Venneti, K., Ponsudha, P., Kushwaha, S., & Kalpana, P. E. (2023). Integrated project for data communication in wireless sensor network. In Proceedings of the IEEE 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-5). India.
[16] Kushwaha, S., S, S., Hariharan, G., Vidhya, K., Reddy, R. V. K., & Madan, P. (2023). Kohonen self-organizable maps based classification of optical code division multiple access codes. In Proceedings of the 2023 International Conference on Inventive Computation Technologies (ICICT) (pp. 1580-1584). Lalitpur, Nepal.
[17] Raviraja, S., Seethalakshmi, K., Kushwaha, S., Priya, V. P. M., Kumar, K. R., & Dhyani, B. (2023). Optimization of the ART tomographic reconstruction algorithm - Monte Carlo simulation. In Proceedings of the 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 984-988). Salem, India.
[18] Kumar, V., & Kushwaha, S. (2023). Map-Reduce task scheduling optimization techniques: A comparative study. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 729-736). Tirunelveli, India.
[19] Kushwaha, S. (2023). A futuristic perspective on artificial intelligence. In Proceedings of the IEEE OPJU International Technology Conference on Emerging Technologies For Sustainable Development (pp. 1-6). O.P. Jindal University, Raigarh, Chhattisgarh, India.
[20] Kushwaha, S. (2023). Review on artificial intelligence and human computer interaction. In Proceedings of the IEEE OPJU International Technology Conference on Emerging Technologies For Sustainable Development (pp. 1-6). O.P. Jindal University, Raigarh, Chhattisgarh, India.
[21] Gupta, S., Verma, S. K., Samanta, S., Khatua, S., & Kushwaha, S. (2022). Prospect of Li-ion battery in designing environment friendly hybrid electric vehicles. In Proceedings of the International Conference on Advanced Earth Sciences & Foundation Engineering (ICASF-2022) (Vol. 1110, pp. 1-8). Chandigarh University, Punjab, India.
[22] Kushwaha, S., Jayaprakash, M., Swamy, V. K., Senthil, V., Maddila, S. K., & Anusuya, M. (2022). Design and development of communication networks using IoT. In Proceedings of the International Conference on Materials, Computing, Communication Technologies (ICMCCT 2022) (pp. 275-283). Cheran College of Engineering, Karur, Tamilnadu, India. ISBN: 9788770229555.
[23] Kumar, V., & Kushwaha, S. (2022). An optimized job scheduling mechanism for MapReduce framework using DIW-WOA in big data. In Proceedings of the IEEE International Conference on Knowledge Engineering and Communication Systems (ICKECS-2022) (pp. 1-8). SJC Institute of Technology, Chickballapur, Karnataka, India.
[24] Mohan, M., Patil, A., Mohana, S., Subhashini, P., Kushwaha, S., & Pandian, S. M. (2022). Multi-tier kernel for disease prediction using texture analysis with MR images. In Proceedings of the IEEE International Conference on Edge Computing and Applications (ICECAA 2022) (pp. 1020-1024). Gnanamani College of Technology, Namakkal, Tamilnadu, India. ISBN: 978-1-6654-8232-5.
[25] Lee, S. H. (2019). A Study on Cloud-Based IoT Systems for Real-Time Data Monitoring. IEEE Transactions on Cloud Computing, **7(3)**, 430-438.
[26] Kushwaha, S. (2025). Practical IoT Solutions for Students Using Popular Development Platforms: Arduino, Raspberry Pi and NodeMCU (1st ed.). Eliva Press. ISBN: 978-99993-2-454-0.
[27] Kushwaha, S. (2024). Research Methodology (1st ed.). Eliva Press. ISBN: 978-99993-2-155-6.
[28] Kushwaha, S. (2023). Internet of Things (IoT) with Arduino Uno, Raspberry Pi & NodeMCU (1st ed.). Notion Press. ISBN: 9798892331265.
[29] Kushwaha, S. (2023). Challenges and opportunities in the development of a smart grid system in India. In Big Data Analytics Framework for Smart Grids (1st ed., pp. 1-15). CRC Press. ISBN: 9781032665399.
[30] Kumar, V., Kushwaha, S., Yadav, S., Sharma, A., Barik, R. K., & Gupta, M. K. (2023). A review on Internet of Multimedia Things (IoMT): Communication techniques perspective. In 5G and Beyond Wireless Networks Technology, Network Deployments and Materials Used for Antenna Deployments (1st ed., pp. 1-246). CRC Press. ISBN: 9781032504803.
[31] Antony, A. S. M., Hanumanthakari, S., Kumar, A., & Kushwaha, S. (2022). Soft Computing (1st ed.). Scientific International Publishing House. ISBN: 978-93-5625-566-1.
[32] Kushwaha, S. (2021). Enhancement of Color Images (1st ed.). Notion Press. ISBN: 9781638063209.
[33] Kushwaha, S. (2021). Hybrid Methods for Speckle Noise Denoising in Ultrasound Images (1st ed.). Notion Press. ISBN: 9781638062097.

[34] Kushwaha, S. (2019). Artificial intelligence fundamentals for intelligent market analysis. In Paradigms of New Age Marketing (pp. 79-86). National Press Associates. ISBN: 978-93-85835-66-7.
[35] Alashjaee, A. M., Kushwaha, S., Alamro, H., Hassan, A. A., Alanazi, F., & Mohamed, A. (2024). Optimizing 5G network performance with dynamic resource allocation, robust encryption, and Quality of Service (QoS) enhancement. PeerJ Computer Science, 10, e2567.
[36] Kushwaha, S., Chithras, T., Girija, S. P., Prasanth, K. G., Minisha, R. A., Dhanalakshmi, M., Jayanthi, A., Robin, C. R. R., & Rajaram, A. (2024). Efficient liver disease diagnosis using infrared image processing for enhanced detection and monitoring. Journal of Environmental Protection and Ecology, 25(4), 1266–1278.
[37] Bharadwaj, H. K., Agarwal, A., Chamola, V., Lakkaniga, N. R., Hassija, V., Guizani, M., & Sikdar, B. (2021). A review on the role of machine learning in enabling IoT based healthcare applications. *IEEE Access, 9*, 38859–38890.
[38] Vimal, S. P., Vadivel, M., Baskar, V. V., Sivakumar, V. G., & Srinivasan, C. (2023). Integrating IoT and machine learning for real-time patient health monitoring with sensor networks. In *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 574–578).
[39] Ganesan, M., & Sivakumar, N. (2019). IoT based heart disease prediction and diagnosis model for healthcare using machine learning models. In *2019 IEEE international conference on system, computation, automation and networking (ICSCAN)* (pp. 1–5). IEEE.
[40] Sworna, N. S., Islam, A. M., Shatabda, S., & Islam, S. (2021). Towards development of IoT-ML driven healthcare systems: A survey. *Journal of Network and Computer Applications, 196*, 103244.
[41] Yıldırım, E., Cicioğlu, M., & Çalhan, A. (2023). Fog-cloud architecture-driven internet of medical things framework for healthcare monitoring. *Medical & Biological Engineering & Computing, 61*, 1133–1147.
[42] Yaqoob, M.-M., Khurshid, W., Liu, L., Arif, S.-Z., Khan, I.-A., Khalid, O., & Nawaz, R. (2022). Adaptive multi-cost routing protocol to enhance lifetime for wireless body area network. *Computational Materials and Continua, 72*, 1089–1103.
[43] Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computers and Communications, 153*, 311–335.
[44] Amzil, A., Abid, M., Hanini, M., Zaaloul, A., & El Kafhali, S. (2024). Stochastic analysis of fog computing and machine learning for scalable low-latency healthcare monitoring. *Cluster Computing, 27*, 6097–6110.
[45] Chi, H. R., Domingues, M. d. F., Zhu, H., Li, C., Kojima, K., & Radwan, A. (2023). Healthcare 5.0: The perspective of consumer internet-of-things-based fog/cloud computing. *IEEE Transactions on Consumer Electronics, 69*, 745–755.
[46] Nazarian, S., Glover, B., Ashrafian, H., Darzi, A., & Teare, J. (2021). Diagnostic accuracy of artificial intelligence and computer-aided diagnosis for the detection and characterization of colorectal polyps: Systematic review and meta-analysis. *Journal of Medical Internet Research, 23*, e27370.
[47] Lakhan, A., Mohammed, M. A., Kozlov, S., & Rodrigues, J. J. (2024). Mobile-fog-cloud assisted deep reinforcement learning and blockchain-enable IoMT system for healthcare workflows. *Transactions on Emerging Telecommunications Technologies, 35*, e4363.
[48] Konno, N., & Schillaci, C. E. (2021). Intellectual capital in Society 5.0 by the lens of the knowledge creation theory. *Journal of Intellectual Capital, 22*, 478–505.
[49] Yaqoob, M. M., Nazir, M., Yousafzai, A., Khan, M. A., Shaikh, A. A., Algarni, A. D., & Elmannai, H. (2022). Modified artificial bee colony based feature optimized federated learning for heart disease diagnosis in healthcare. *Applied Sciences, 12*, 12080.
[50] Khan, M. A., Alsulami, M., Yaqoob, M. M., Alsadie, D., Saudagar, A. K. J., AlKhathami, M., & Farooq, K. U. (2023). Asynchronous federated learning for improved cardiovascular disease prediction using artificial intelligence. *Diagnostics, 13*, 2340.