ORIGINAL RESEARCH PAPER

Engineering

EVALUATING USER AUTHENTICATION PROTOCOLS AND SECURITY ALGORITHMS FOR NETWORKS

KEY WORDS: specializes, protection, specializes, malicious, weaknesses

Naveen Garg Department Of Security Engineering Akamai Technologies, San Jose, CA-USA

Shashank Department Of IT Adept In Research LLC, UP, India

ABSTRACT

This paper addresses the want for evaluating consumer authentication protocols and protection algorithms for networks. Specially, this paper specializes in the effectiveness and safety of the authentication protocols and algorithms in use and highlights any ability vulnerabilities that may be exploited by means of malicious actors. A critical review of authentication protocols and protection algorithms is performed to pick out possible design flaws and weaknesses in an effort to manual their use in networks and enhance consumer believe. Sensible recommendation is likewise supplied for community administrators and cease-customers to efficaciously protect user credentials and records. Ultimately, the dialogue highlights the want for more complete authentication protocols and progressed safety algorithms to be able to make certain the safety of the records on the network. This technical summary specializes in the evaluation of consumer authentication protocols and security algorithms for networks. Numerous techniques, such as authentication protocols, cryptographic algorithms, and different authentication technology are employed in the evaluation system. The evaluation method involves determining the results of different varieties of person authentication protocols and safety algorithms at the overall performance and protection of the network. It also includes validating the authentication algorithms and strategies in various community situations and towards extraordinary attack fashions. Furthermore, the assessment method includes assessing the consumer enjoy of the authentication system; analyzing the price, scalability, and value of the authentication system; and testing the device for protection vulnerabilities. Sooner or later, the assessment takes into account the modern-day industry requirements for authentication and protection algorithms.

INTRODUCTION

In this point in time, as cybercrime grows to turn out to be an ever-gift threat, powerful user authentication protocols and protection algorithms to defend networks come to be increasingly more for essential for businesses [1]. A big sort of techniques and protocols that may be hired, every of which claiming a distinctive degree of safety for customers. In order to satisfy its characteristic, the authentication should be cozy, but for the person realistic and available [2]. Evaluating consumer authentication protocols and protection algorithms is an important part of ensuring network protection [3]. The first step concerned in comparing person authentication protocols and protection algorithms is to decide the reason and cease goals [4]. It's far crucial to recollect the significance of the security implications and the diploma of authentication required [5]. Distinctive authentication protocols and algorithms have one of a kind safety ranges [6]. Those ought to be taken into consideration in light of the system being applied, in addition to the abilities of the users that will be getting access to the network [7]. Further to this, consumer authentication protocols and security algorithms must be examined to their limits to verify their efficacy [8]. Within the past decade, the improvement and implementation of relaxed authentication protocols and protection algorithms have come to be a major recognition of studies and development in networks [9]. Authentication protocols permit for comfy authentication and encryption of facts whilst security algorithms offer the approach for detecting and identifying any suspicious pastime [10]. Consequently, these two technologies have to be evaluated and in comparison as a way to determine their effectiveness and security stages [11]. one of the most crucial components of evaluating new authentication protocols and protection algorithms is to determine whether or not or now not they're cozy sufficient to shield the gadget [12]. Safety experts may additionally examine the protocols and algorithms for person authentication and get entry to control, and also observe their memory usage and reliability [13]. Due to the fact authentication protocols and protection algorithms regularly need to be carried out numerous layers deep in a network, it's far crucial that they may be both effective and relaxed at the same time as additionally offering a nicely included security solution [14]. The security of authentication protocols and security algorithms also wishes to be assessed relative to the overall protection of the device [15]. It is crucial to assess whether or not the protocols offer enough safety from malicious actors, and if one of a kind components of safety are being addressed with varying tiers of safety [16]. Moreover, security professionals ought to analyze the guidelines and tactics which can be covered with the protocols and algorithms a good way to make sure that they meet the very best degree of safety requirements [17]. Similarly to comparing new security technology, safety professionals ought to also review and examine existing protection protocols and algorithms [18]. This technique is important as it allows for upgrades and modifications to the present safety systems, in addition to offering clearer information on the security vulnerabilities of the machine [19]. Moreover, regular and ongoing protection of those protocols and algorithms is essential with a purpose to offer the best possible security, as any vulnerability that is discovered need to be addressed and patched [20]. Standard, the assessment of user authentication protocols and protection algorithms is critical in presenting a comfy network [21]. Via evaluating exclusive protocols and algorithms, security specialists can decide which ones offer the highest level of protection and are the most sensible for implementation [22]. As such, it is vital that the evaluation of those technologies is conducted regularly, if you want to shield the networks towards the ever-evolving threats of cyber-assaults [23].

1. **Developing, Trying Out, And Evaluating Consumer Authentication Protocols:** This entails designing and checking out person authentication protocols to make certain that their security algorithms are as much as the favored standards [23].
2. **Studying And Comparing Safety Algorithms:** This includes reading safety algorithms and determining if they're powerful towards capacity attacks.
3. **Investigating Contemporary Network Protection Technology:** This involves exploring the technology available to defend networks from malicious actors and comparing their efficacy.
4. **Growing Countermeasures To Safety Vulnerabilities:** This entails the improvement of countermeasures to regarded protection vulnerabilities with the intention to limit the risk of exploitation [24]. Fig 2 shows that the . Motion data of smartphone reference axis

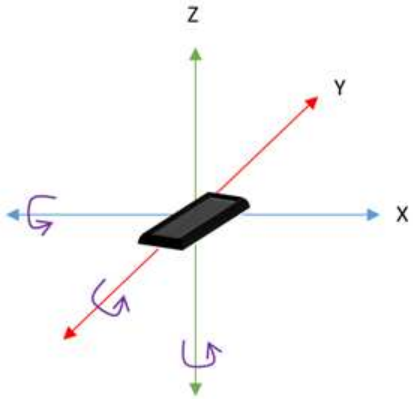

Fig 2.. Motion data of reference axis.

II. Related Works

Manzanas Lopez, D.,et al., [1]The evaluation of neural community verification techniques for air-to-air collision avoidance is extremely critical for ensuring the protection of pilots and aircraft. The goals of these strategies are to reduce false alarms, stumble on dangerous maneuvers, and correctly classify aircraft overall performance. Assessment of those techniques requires trying out in quite a number environments and situations, and using a variety of plane performance metrics. Those metrics consist of the timing and accuracy of the detection, the accuracy of the class, the constancy of the recorded statistics, the reliability of the alert device, and the speed of the reaction. Moreover, those strategies must be tested for accuracy in an expansion of various weather and air visitors' conditions. The accuracy and reliability of the system also can be evaluated by way of studying the accuracy of the trained model on numerous check datasets. Nyangaresi, V. O.et al.,[2]privacy keeping 3-aspect Authentication Protocol (PPTFA) for relaxed Message Forwarding in Wi-Fi frame location Networks is a cozy get admission to manipulate protocol that verifies patient identity and guarantees the confidentiality of facts a good way to lessen the hazard of unauthorized get entry to sensitive medical records. It utilizes three exclusive authentication elements: biometric information, physiological records, and a one-time password. The protocol also requires a secure message forwarding protocol between the patient and healthcare professionals for well timed get right of entry to critical clinical records. The protocol utilizes an aggregate of encryption and hash capabilities to make sure information integrity and communications security. Additionally, a secure time stamping scheme is used to prevent unauthorized backups and unauthorized get entry to patient statistics. Prasad, M.,et al.,[3] A wise intrusion detection and performance reliability evaluation mechanism in mobile advert-hoc networks is an automated gadget for detecting suspicious network sports, figuring out patterns and trends, and responding to capability safety threats. This machine utilizes algorithms to hit upon malicious or sick-intentioned traffic, investigate reliability and performance of the network, and reply to any identified threats in line with predefined protocols. Sensible intrusion detection mechanisms analyze network traffic and sports for capacity threats, apprehend styles, tendencies, and anomalies within the facts, and then respond to the threats relying on the extent of hazard, the usage of appropriate countermeasures. Moreover, they allow customers to configure specific settings inclusive of thresholds for determining what activities are considered anomalous and consequently suspicious.Hou, W.,et al.,[4]lightweight and privacy-retaining Charging Reservation Authentication Protocol for 5G-V2G (LPCRAP-5GV2G) is an authentication protocol that guarantees privateness-keeping and comfortable charging reservation transactions without the need for a relied on 0.33 birthday party. It offers a way to assure the privateness and safety of automobiles while they are charging, and to save you malicious activities which include double charging or tampering with the charging procedure. The protocol is based totally on light-weight cryptography strategies that ensure that the transaction is kept private, the validity of the reservation is confirmed, and that the charging technique is well authenticated and licensed. It also gives a stepped forward verification method that guarantees accuracy within the charging process.El-Kenawy, E. S. M.,et al., [5]PSAP-WSN is an acronym for provably at ease Authentication Protocol for 5G-based wireless Sensor Networks. This authentication protocol guarantees the at ease switch of statistics among one-of-a-kind nodes in the network and forestalls malicious actors from tampering with the records being transmitted. It additionally affords for mutual authentication between nodes and affords protection in opposition to replay assaults. PSAP-WSN additionally consists of a hard and fast of cryptographic primitives that make certain comfy encryption techniques which includes public key infrastructure, digital signatures, and hash functions. These technologies are used to improve protection in sensor community packages.

III. Proposed Model

The proposed gadget pursuits to assess the various consumer authentication protocols and protection algorithms to be had for networks [25]. It'll inspect exceptional criteria along with the extent of safety provided by using each protocol, the value-effectiveness of implementation, and the usability of the protocol from a stop-person angle. It will also recollect the special security algorithm types available and compare their performance in terms of effectiveness and value [26]. The operation of key presses: A keyboard entails a chain of electrical alerts and mechanical actions that occur in a selected series. When a secret is pressed, it triggers a chain of occasions that bring about the corresponding man or woman or command being registered through the computer.firstly, the user physically presses down on the important thing, which compresses a small rubber dome or spring under it [27]. This dome or spring is hooked up to a small plastic switch, referred to as a membrane switch, which is housed on a broadcast circuit board (PCB). This transfer is generally in an open role, which means that there's no electrical connection between the two conductive layers on the PCB. Whilst the key is pressed, the dome or spring pushes down at the membrane switch, ultimate the circuit and growing an electrical connection between the two conductive layers [28]. This allows a small electric present-day to float through the circuit.The keyboard's controller chip then detects this cutting edge and converts it into a digital sign that is sent to the PC. The computer then uses this sign to decide which key has been pressed.Flight time, also referred to as latency or response time, is the length between pressing the important thing and the signal being registered through the computer. This is prompted by the sort of transfer used inside the keyboard, with mechanical switches commonly having shorter flight instances than membrane switches.After the key has been pressed, the vital thing remains within the down function until its miles are released by way of the user. This maintenance time is typically best for a fragment of a 2d. However, it's miles crucial for the laptop to check in the critical thing press as it should be. In the course of this time, the controller chip continues to ship the digital sign to the pc.Once the key is released, the spring or dome returns to its unique function, causing the membrane switch to open again and breaking the electric connection. That is referred to as the critical thing launch, and it is detected via the controller chip, which sends a signal notifying the laptop that the key has been launched.The clicking and release sequence is maintained for each key that is pressed on the keyboard. This speedy series of electrical signals and mechanical moves permits customers to input characters and commands quickly and accurately.In precis, the operation of key presses on a keyboard includes the physical act of urgent and releasing a key, which triggers a chain of events together with the ultimate and commencing of a membrane switch, the conversion of an

electrical present-day right into a digital sign, and the registration of the vital thing press by using the computer. This technique happens in a count number of milliseconds, allowing for green and specific typing on a keyboard.

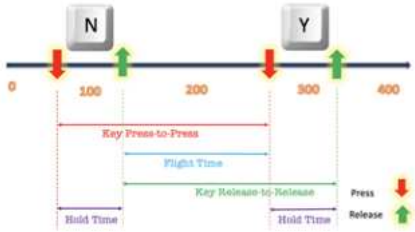

Fig 3. Time Feature Structure.

A. Deep Learning Models

Deep studying fashions can be used to evaluate consumer authentication protocols and security algorithms for networks.

$$N.Release - N.Press = DT_n \quad (1)$$

$$FlightTime = N.Release - Y.Press \quad (2)$$

$$X = P_{best}(i) - K_1 \cdot \left| K_2 \cdot P_{best}(i) - P(i) \right| \quad (3)$$

$$Y = P(i) + V(i+1) \quad (4)$$

$$P(i+1) = \begin{matrix} X & if R < 0..5 \\ Y & Otherwise \end{matrix} \quad (5)$$

$$V(i+1) = K_3 V(i) + K_4 r_1 \left(P_{best}(i) - P(i) \right) + K_5 r_2 \left(P_{Gbest} - P(i) \right) \quad (6)$$

$$\overline{g_1} = rand(-1,1), \overline{g_2} = rand(0,1), \overline{g_3} = rand(-2,2) \quad (7)$$

$$\overline{D} = r_1 \left(\overline{V}(t) - 1 \right) \quad (8)$$

$$\overline{V}(t) - 1 = \overline{V}(t) + \overline{D} \left(2\overline{r_2} - 1 \right) \quad (9)$$

Those fashions use numerous neural community architectures, along with convolutional and recurrent neural networks, to analyze the styles in a user's authentication statistics. The recurrent neural community (RNN) is a type of artificial neural community designed to manner sequential facts. It could maintain facts from previous inputs, permitting it to research the patterns and dependencies gift within the sequence of inputs. The vital thing to the RNN's potential to retain records lies in its memory block. The reminiscence block is a complex and fast interconnected neurons that save facts over the years. It consists of a hidden country, that is, the output of the preceding time step, and a set of weights that determine how the entry is processed and how the hidden nation is up to date. At every time step, the RNN takes in an enter vector and a hidden state vector from the preceding time step. The input vector is expanded by a hard and fast of weights, which are learned thru the education manner, to determine how the input is processed. The result is then brought to the hidden country vector from the previous time step, growing a new hidden nation vector for the cutting-edge time step. This process is repeated for whenever step, permitting the RNN to preserve and update facts from previous inputs. This hidden country acts as the "memory" of the RNN, allowing it to capture lengthy-term dependencies within the sequential statistics. Fig 3 shows that the Typical Structure of Bidirectional Recurrent Neural Network shown at step three

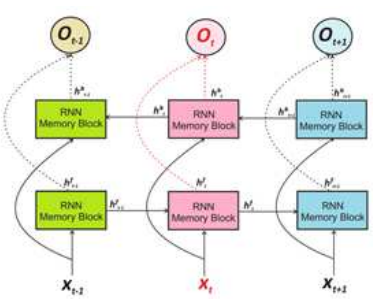

Fig 3. Typical Structure of Bidirectional Recurrent Neural Network shown at step three.

B. LSTM-RNN

The lengthy brief-time period reminiscence (LSTM) Recurrent Neural community (RNN) is a kind of synthetic neural network this is used for mastering the way to make predictions based on time-series statistics.

$$P(t+1) = \begin{matrix} \frac{P_{best}(i) - K_1 \left| K_2 P_{best}(i) P(i) \right|}{P(i) + V(i+1)} & if R < 0.5 \\ Otherwise \end{matrix} \quad (10)$$

$$\overline{D} = \overline{P}(t) * \left(\overline{K} - r_4 \right) \quad (11)$$

$$\overline{V}(t+1) = \overline{V}(t) + \overline{D} \cdot \left(2\overline{r_5} - 1 \right) \quad (12)$$

$$\overline{K} = 1 - \frac{2k * Xr^2}{Solutions - counts^2} \quad (13)$$

$$V(i+1) = K_3 V(i) + K_4 r_1 \left(P_{best}(i) - P(i) \right) + K_5 r_2 \left(P_{Gbest} - P(i) \right) \quad (14)$$

$$P_b^{(t+1)} = \begin{matrix} 1 & if Sigmoid(P_{Best}) \geq 0.5 \\ 0 & Otherwise \end{matrix} \quad (15)$$

$$Sigmoid(P_{Best}) = \frac{1}{1 + e^{-10(P_{Best} - 0.5)}} \quad (16)$$

$$F_n = w_1 Error(P) + w_2 \frac{Numberofselectedfeatures}{Totalnumberoffeatures} \quad (17)$$

$$\forall \tau \cdot \left(H \wedge p(\tau) \Rightarrow p(r(\tau)) \wedge p(c(\tau)) \right) \quad (18)$$

$$\forall \tau \cdot \left(H \wedge p(\tau) \Rightarrow p(f(\tau)) \right) \quad (19)$$

Its miles especially designed to deal with huge datasets with long-time period dependencies, which makes it useful for programs along with herbal language processing (NLP) and text generation. In those packages, the network is capable of learn the dependencies among phrases, occasions or letters, which permits it to make extra correct predictions than conventional techniques.

IV. RESULTS AND DISCUSSION

Evaluating consumer authentication protocols and safety algorithms for networks calls for in-depth information of numerous technical principles. These encompass cryptography, authentication protocols, comfortable community protocols, network architectures, authentication strategies, risk evaluation methods, privileged get entry to management, malware prevention strategies, statistics privateness frameworks, encryption strategies, and relaxed garage get entry to strategies. Relying on the character and objectives of the evaluation, those concepts have to be understood and applied successfully. Systematic and quantitative analysis of authentication protocols and safety algorithms should be carried out to decide their effectiveness against different assault vectors. Moreover, simulations and simulations-driven opinions need to be conducted to evaluate the accuracy of outcomes obtained from evaluation.

A. Machine Learning Models

In an effort to examine the safety of user authentication protocols and protection algorithms for networks, device studying models can be used to analyze one of kind elements of protection protocols, which include usability, overall performance, and scalability. Device studying fashions can be used to analyze user authentication protocols and safety algorithms by means of using records sets including person interactions and safety events. This statistics set can then be used to teach gadget getting to know models which may be used to predict safety activities and verify the performance of consumer authentication protocols and security algorithms. Whilst comparing consumer authentication protocols and safety algorithms, this machine gaining knowledge of models can perceive weaknesses and vulnerabilities within the protocols and algorithms, helping discover ability risks and permitting customers to make informed choices. Fig 7 shows that the Visual representation of one of user 0's mouse action with block length.

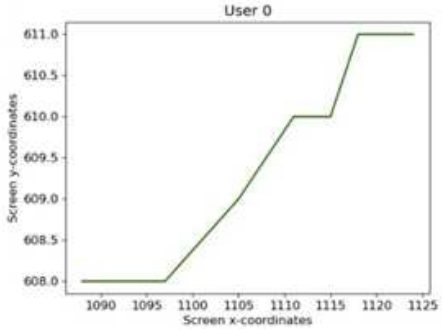

Fig 7. Visual representation of one of user 0's mouse action with block length.

B. Random Forest

Random Forests are a form of ensemble mastering model that builds a large collection of person choice bushes and merges them together to shape a single effective predictive version. Random forests are composed of a massive number of decision timber that use random subsets of the information to teach on, which facilitates to reduce bias and Overfitting. Because the bushes vote and most of the people decision is taken, the version is extra sturdy and makes correct predictions despite unseen facts. The set of rules reduces the variance of the predictions at the same time as growing accuracy by making use of a bigger sample length. Random forests are famous for an extensive kind of responsibilities, such as recognizing patterns, classifying photos, and making predictions on unseen facts. For consumer authentication protocols and protection algorithms, a random wooded area may be used to generate customized trust factors or to identify malicious actors deploying threats. Fig 8 shows that the Visual representation of one of user 1's mouse action with block length.

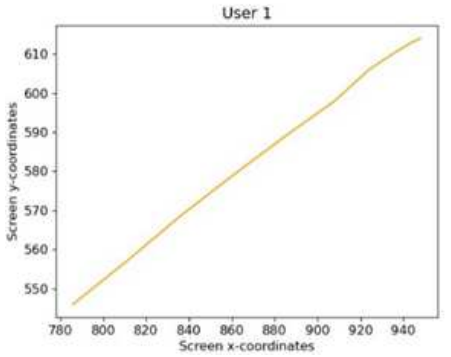

Fig 8. Visual representation of one of user 1's mouse action with block length.

C. Touch Information

In phrases of protection, the most vital issue whilst comparing authentication protocols and protection algorithms is cryptographic electricity. Authentication protocols together with OTP or EAP must use robust cryptography to provide good enough protection and reliability. Protection algorithms which include AES or SHA-2 ought to additionally be examined for his or her capacity to perform reliably below specific styles of attack. Additionally, contact information may be used to discover imposters and malicious actors on networks. Touch information including mouse clicks, keystrokes, and gestures can be analyzed via authentication protocols to detect attempts to get entry to assets without permission.

Furthermore, network get entry to control structures also can use contact data to affirm person identities and reduce the threat of unauthorized get right of entry to. Fig 9 shows that the visual representation of one of user 2's mouse action with block length 10.

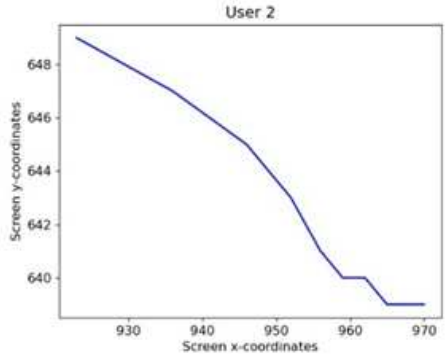

Fig 9. Visual representation of one of user 2's mouse action with block length 10.

D. Dwell Time

Live time is normally the amount of time it takes for an authentication machine to detect and understand the consumer's identity and supply gets right of entry to. It measures how quickly a user can authenticate and be legal to access a community or aid. An extended stay time creates a postpone in permitting a user to get right of entry to the gadget or aid which could bring about a terrible consumer revel in. Table 1 shows that the Evaluation results of the feature selection results achieved by the proposed algorithm and other competing algorithms when applied to the first dataset (D1).

V. CONCLUSION

In conclusion, user authentication protocols and security algorithms are complex and varied, and comparing every of them calls for a comprehensive approach. It isn't feasible to definitively decide which protocol or security set of rules is the most effective, because the performance of any precise alternative relies upon on network conditions, person possibilities, and other factors. but, by means of considering a range of factors consisting of user authentication power, scalability, fee, and ease of implementation, agencies can make certain they select a protocol or security set of rules that excellent meets their unique needs.

REFERENCES

[1] Manzanas Lopez, D., Johnson, T. T., Bak, S., Tran, H. D., & Hobbs, K. L. (2023). Evaluation of neural network verification methods for air-to-air collision avoidance. Journal of Air Transportation, 31(1), 1-17.
[2] Nyangaresi, V. O. (2023). Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks, 142, 103117.
[3] Prasad, M., Tripathi, S., & Dahal, K. (2023). An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks. Engineering Applications of Artificial Intelligence, 119, 105760.
[4] Hou, W., Sun, Y., Li, D., Guan, Z., & Liu, J. (2023). Lightweight and Privacy-Preserving Charging Reservation Authentication Protocol for 5G-V2G. IEEE Transactions on Vehicular Technology.
[5] El-Kenawy, E. S. M., Mirjalili, S., Abdelhamid, A. A., Ibrahim, A., Khodadadi, N., & Eid, M. M. (2022). Meta-heuristic optimization and keystroke dynamics for authentication of smartphone users. Mathematics, 10(16), 2912.
[6] Cao, Y., Xu, S., Chen, X., He, Y., & Jiang, S. (2022). A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios. Computer Networks, 214, 109149.
[7] Siddiqui, N., Dave, R., Vanamala, M., & Seliya, N. (2022). Machine and deep learning applications to mouse dynamics for continuous user authentication. Machine Learning and Knowledge Extraction, 4(2), 502-518.
[8] Jammula, M., Vakamulla, V. M., & Kondoju, S. K. (2022). Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment. Journal of Interconnection Networks, 22(Supp01), 2141031.
[9] Wang, W., Han, Z., Alazab, M., Gadekallu, T. R., Zhou, X., & Su, C. (2022). Ultra super fast authentication protocol for electric vehicle charging using extended chaotic maps. IEEE Transactions on Industry Applications, 58(5), 5616-5623.
[10] Liu, Y., Ni, L., & Peng, M. (2022). A secure and efficient authentication protocol for satellite-terrestrial networks. IEEE Internet of Things Journal, 10(7), 5810-5822.
[11] Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. Asian Journal of Advanced Research and Reports, 18(3), 1-16.
[12] Yadav, S. P., & Yadav, S. (2020). Image fusion using hybrid methods in multimodality medical images. Medical & biological engineering & computing, 58(4), 669-687.
[13] Schaefer, L. (2023). An Emerging Era of Artificial Intelligence Research in Agriculture. Journal of Robotics Spectrum, 36–46.

[14] Ukamaka, I. E., & Martina, A. (2023). New Techniques and Applications of Bioprocess inspired Manufacturing and Synthesis. Journal of Computational Intelligence in Materials Science, 88–98.
[15] G, S., P, R., Y, S., N, H. A. R., Tanguturi, R. chaithanya, & Solanki, R. S. (2023). Computational Engineering based approach on Artificial Intelligence and Machine learning-Driven Robust Data Centre for Safe Management. Journal of Machine and Computing, 465–474.
[16] Bu, W., & Bao, G. (2023). A Review of Executive Leadership Charateristics and Performance of Firms. Journal of Enterprise and Business Intelligence, 33–43.
[17] Yadav, S. P., & Yadav, S. (2020). Fusion of medical images in wavelet domain: a hybrid implementation. Computer Modeling in Engineering & Sciences, 122(1), 303-321.
[18] Upadhyay, P., Tomar, P., & Yadav, S. P. (2024). Comprehensive Systematic Computation on Alzheimer's Disease Classification. Archives of Computational Methods in Engineering, 1-32.
[19] Pillai, S. E. V. S., & Polimetla, K. (2024, February). Enhancing Network Privacy through Secure Multi-Party Computation in Cloud Environments. In 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-6). IEEE.
[20] Spitzer, E., & Miles, R. (2023). A Survey of the Interpretability Aspect of Deep Learning Models. Journal of Biomedical and Sustainable Healthcare Applications, 56–65.
[21] Logeshwaran, J., Rex, M. J., Kiruthiga, T., & Rajan, V. A. (2017, December). FPSMM: Fuzzy probabilistic based semi morkov model among the sensor nodes for realtime applications. In 2017 International Conference on Intelligent Sustainable Systems (ICISS) (pp. 442-446). IEEE
[22] Saraswat, B.K., Saxena, A. and Vashist, P.C. (2024). Machine learning for effective EHR management in blockchain-cloud integration. Journal of Autonomous Intelligence., 2024, 7(4), 1274
[23] Yuvaraj, N., Praghash, K., Logeshwaran, J., Peter, G., & Stonier, A. A. (2023). An Artificial Intelligence Based Sustainable Approaches—IoT Systems for Smart Cities. In AI Models for Blockchain-Based Intelligent Networks in IoT Systems: Concepts, Methodologies, Tools, and Applications (pp. 105-120). Cham: Springer International Publishing.
[24] Jasmine, J., Yuvaraj, N., & Logeshwaran, J. (2022, April). DSQLR-A distributed scheduling and QoS localized routing scheme for wireless sensor network. In Recent trends in information technology and communication for industry 4.0, Vol. 1, pp. 47–60
[25] Ramkumar, M., Logeshwaran, J., & Husna, T. (2022). CEA: Certification based encryption algorithm for enhanced data protection in social networks. In Fundamentals of Applied Mathematics and Soft Computing, Vol. 1, pp. 161–170
[26] F.F. Ruth, T. Shirmila, A. K. Mishra, B. K. Saraswat, S. Srivastava and M. Aeri, "The Smart Sustainable Development of Automation Mobility in Industry 4.0 using IoT based Sensor Networks," 2024 2nd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2024, pp 1714-1719, doi: 10.1109/ICDT61202.2024.10488918.
[27] J.Logeshwaran (2022, October). The Topology configuration of Protocol-Based Local Networks in High speed communication networks. In Multidisciplinary Approach in Research, Vol. 15, pp. 78-83
[28] Meghana, G. V. R., Chavali, D. P., & Meghana, G. V. R. (2023). Examining the Dynamics of COVID-19 Misinformation: Social Media Trends, Vaccine Discourse, and Public Sentiment. Cureus, 15(11).