Implementation of a Machine Learning-based Trust Management System in Social Internet of Things

Dr. Chandrashekhar Goswami
Associate Professor
Amity University
Gwalior, Madhya Pradesh, India
shekhar.goswami358@gmail.com

Dr. Ramakrishnan Raman
Professor and Director
Symbiosis Institute of Business Management
Pune & Symbiosis International (Deemed University)
Pune, Maharashtra, India
raman06@yahoo.com

Dr. Biju G. Pillai
Director - BIIB & Dean - Faculty of Management
Department of IT & Business Analytics
Sri Balaji University
Pune (SBUP)
bijupillai@sbup.edu.in

Rajesh Singh
Uttaranchal Institute of Technology
Uttaranchal University
Dehradun, Uttarakhand, India
drrajeshsingh004@gmail.com

Basava Dhanne
Assistant Professor
Electronics and Communication Engineering
St. Matrins Engineering College
Secunderabad, Hyderabad Telangana.
basavaece@smec.ac.in

Dr. Dhiraj Kapila
Associate Professor
Department of Computer Science & Engineering,
Lovely Professional University
Phagwara, Punjab, India
dhiraj.23509@lpu.co.in

2022 5th International Conference on Contemporary Computing and Informatics (IC3I) | 979-8-3503-9826-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/IC3I56241.2022.10072551

***Abstract*- IoT (Internet of Things) is a constantly expanding network made up of billions of connected physical things, including many sensors, embedded devices, smartphones, and wearables. These actual things are typically referred to as "smart objects." A development of the Internet of Things, the Social Internet of Things (SIoT) combines ideas of social networking to create social networks of linked smart items. They sift through the SIoT looking for services and relevant information. In the early stages of research, the concept of trust and trustworthy in social communities created by SIoT is still relatively new. We outline the foundations of SIoT and the ideas of trust in SIoT while highlighting the parallels and discrepancies between IoT and SIoT. In order to determine an aggregate trust score, all of the trust features are aggregated using a machine learning-based algorithm. Results show that the suggested trust-based model effectively separates the network's trustworthy and untrustworthy nodes.**

Keywords: Machine Learning, Trust Management, Internet of Things (IoT), Social Internet of Things (SIoT).

I. INTRODUCTION

A concept known as the Internet of Things (IoT) enables the connecting of the physical world and the internet through physical items, hence facilitating the creation of intelligent systems and infrastructures. These connected smart physical objects, which include smart watches, sensors, controllers, smartphones, cars, computers, RFID, and other devices, have the ability to interface with each other and work together to achieve a shared objective by using specific addressing schemes and industry-standard communication protocols. This has allowed for a paradigmatic shift in the user experience. Numerous primary applications or areas, including medical services, green framework, shrewd structures and homes, energy, portability and transport, industry and climate/planet, agribusiness, and so forth., may benefit significantly from IoT technologies. Although, the rapidly evolving IoT technology has impressively advanced beyond the typical sensing of immediate surroundings. The issues that forestall the boundless acknowledgment of IoT gadgets and the satisfaction of Iot networks in our regular routines incorporate personal satisfaction, heterogeneity, and versatility [1].

Communities are created in our dynamic, varied, and complex society by utilising social contacts and common interests and powerful needs. Humans connect and work together to find solutions to complicated challenges in their communities. At the point when the possibility of informal organization (social networking) is incorporated into IoT, this reconciliation has led to another worldview called Social-Internet of Things (SIoT), where the shrewd things are advanced into objects with social mindfulness. This worldview expects to effectively take care of the issues of heterogeneity and extensibility, looked by an IoT environment.

Numerous trust the executives' systems and models have been advanced in the exploration for P2P networks [2] and IoT conditions, yet they can't be utilized straightforwardly in SIoT conditions since they are missing social viewpoints and connections between the items as well as friendly trust credits that were not considered. There are as of now only a couple of studies on trust the board in SIoT. The principal study on SIoT trust the board [3] tended to the basic thoughts, qualities, and models set forth for the organization of confidence in SIoT settings yet didn't give a reasonable image of SIoT trust models and trust the executives' frameworks completely. A new report [4] that was delivered in 2019 examined numerous SIoT trust the executives' models and looked at them utilizing different measurements, although it did not examine the most recent SIoT trust management models. Reference [5] have developed and explored in-depth data on IoT and SIoT, featuring their hidden innovations and proposed designs, in another recent survey.

They have investigated, compared, and analysed different trust the executives' frameworks in WSNs and IoT, extricating many highlights from different existing trust the board plans. Be that as it may, this study doesn't give a careful investigation of trust the board frameworks and plans planned explicitly for SIoT conditions. Reference [3] have classified a

rundown of trust and neighborliness based social IoT techniques and described a number of viewpoints, such as the connections between the social IoT and industry 4.0 and the interaction between the social IoT and cloud. However, there is no comparison or investigation of the trust the board solutions suggested regarding SIoT in this paper. The principles of SIoT are described in the most recent study, and thrust areas are also included. The service revelation, relationship the executives, administration sythesis, and trust the board parts of the SIoT ecosystem have been the subject of a study of cutting-edge publications by the authors. They did not, however, compare the most recent trust management methods suggested for the SIoT in their thorough assessment [4].

II. Literature Review

In many different fields, including sociology, history, philosophy, political science, psychology, economics, organizational anagement, computers, automation, international relations, and networking, trust plays a crucial role. Reference [5] defined trust as a level of subjective belief on a specific entity's behaviour. Strategies are created and referred to as "trust management (TM)" for the assessment and development of trust in various frameworks or elements. This phrase was first used by [7], who defined it as a single independent approach used to assess and establish security policies, credentials, and relationships inside the network structure. As a result, while evaluating the behaviour of entities, reliable functionality of the system is kept up with and dangers and vulnerabilities connected with the execution of different administrations are diminished. TM fills in as a promising arrangement when they in view of cryptography are blocked off or neglect to guarantee framework security within the sight of insider, suspicious enemies.

By acting as a moderate layer between requesters of service and suppliers in assistance situated settings like IoT and SIoT, TM advances reliable collaborations and assists with asset the board, access control, dependable service organization, and so forth. Trust is a crucial component of human connections that makes cooperation and collaboration possible. Meanwhile the SIoT worldview looks like human interpersonal organizations and SOs have the ability to manage social interactions by mimicking human natural behaviour, trust is another crucial component of SIoT. For instance, the reliability of an item can be quantified by using the idea of standing. Calculating the propensity of the trustee, the trust worthiness of the trustee, and environmental factors is how trust in SIoT is determined. This process is thought to be abstract and lopsided between the trustor and the legal administrator [6]. In the SIoT, trust models evaluate trust in light of social factors and interpersonal connections. In a SIoT environment, social IoT devices connect with other devices that have similar interests. As a result, communities are created, and relationships grow stronger as a result of more frequent interactions. By social affair both immediate and aberrant conclusions about the service provider (SP) and evaluating the assessed dependability (trust level) of SP, trust models assist decision-making and offer trustworthy recommendations in a particular activity. Once the trust level is over the limit, a transaction is finally completed.

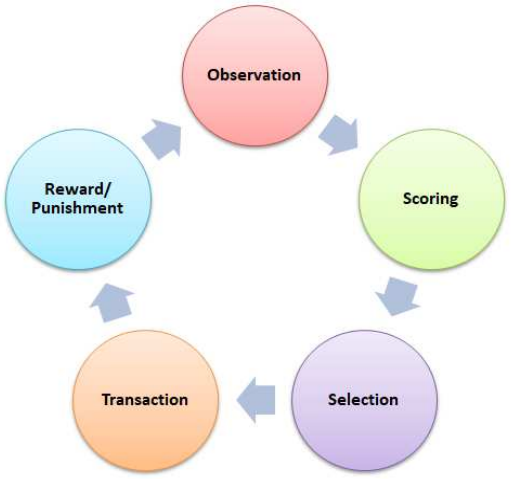

Figure 1: Process of Trust management.

The trust the executive's framework or management of trust utilizes the organization notoriety of articles, the suggestions of adjacent socially associated objects, and authentic conduct as far as conveying administrations or going through with exchanges to break down the way of behaving of SOs in SIoT. Five coordinated stages make up a TM interaction life cycle (likewise portrayed in Fig. 1) and are utilized to control the organization of TM: Perception and information assortment, scoring and trust rating, element determination and trust choice, exchange and trust update, and prize/discipline are the initial four stages. By checking the framework element boundaries and determining the objective discoveries in regards to the substances' dependability, SOs/spectators get information about the articles from which they look for administrations or proposition them administrations in the principal stage. A unified power or a charming specialist or protest will dole out each item in the subsequent stage, following information assortment, a right weight known as notoriety scores. At the point when there are a few items, these standing scores are utilized to rank the things arranged by reliability and needs them. The most proper thing is picked for a specific exchange or IoT administration in light of a bunch of measures after standing scores have been determined. Following item choice, an exchange happens, and for criticism purposes, further information about the article (which has provided the help) is gotten and saved by the framework parts, refreshing the data set considering the experience. At last, different capabilities are utilized to compensate helpful and genuine items with high standing scores locally or all around the world in the organization, while rebuffing malicious and questionable or getting out of hand protests [8]. On the basis of two different types of categories, shown in Fig. 2, we directed a similar investigation of all trust the executives' systems for the IoT. All five of the aforementioned steps of the trust management process are involved. Social trust's various components include its social trust features, assaults, score, and metrics employed by cutting-edge techniques in the literature. For SIoT environments, the trust management process is crucial

since a collection of massive heterogeneous objects may make it difficult to govern the integrity, safety, and security [9].

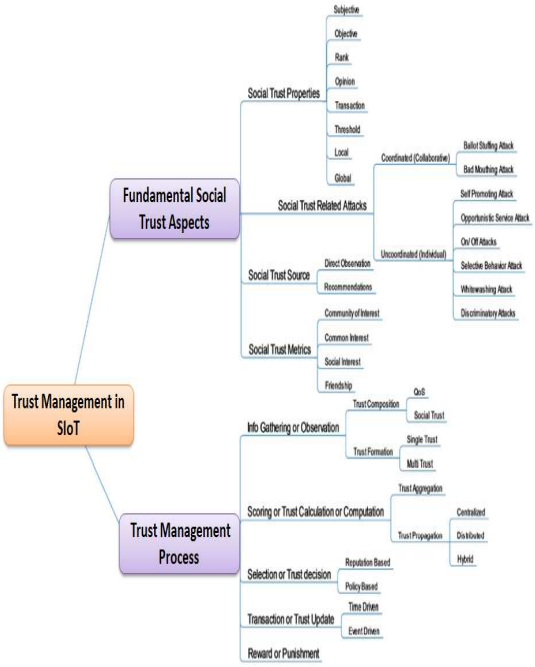

Figure 2: SIoT-Trust Management.

III. METHODOLOGY

The two metrics that make up the trust model in this paper are the Indirect Trust Metric (ITM) and the Direct Trust Metric (DTM), where the former provides the idea of direct observation and the latter offers the standing of hubs in the networking. TX (i, j) stands for the assessment of trust between node I (the trustor) and node j (the trustee), where X stands for social characteristics such friendship likeness, local area of interest, cooperativeness, and rewards. TX (i, j) has a range of [0, 1], where values close to 0 denote lack of trustworthiness and values close to 1 denote trustworthiness. The outcome is saved in the repository and utilized as a score of direct trust after collecting every one of the characters TX (i, j) from the direct interaction using a machine learning-based technique. The node (trustor) asks the other nodes for direct trust in exchange for indirect trust (recommendations). The final trust score is then calculated by combining the two findings (trusts) using Algorithm 1 [2].

A. *Direct Trust Metric (DTM)*

Direct perception of a legal administrator before interaction is provided by DTM. Although there are many various ways to evaluate a trustee, in this paper we have used four primary criteria, which are explained below, to evaluate any trustee in relation to the trustor:

1) Similarity in Friendship: In terms of the interactions between the participating items, friendship similarity represents social relationships. With reference to a particular activity and context, it assesses an object's relative relevance to other objects. This attribute of an item is determined as follows:

$$T_{FS}(i,j) = \frac{|F_i \cap F_j|}{|F_i| - 1} \qquad (1)$$

where |.| denotes the cardinality of a set and Fi and Fj denote a set of friends of nodes I and j, correspondingly.

2) Community-of-Interest (CoI): This type of feature shows how similar two nodes are in terms of the communities or groups of people that share a common social interest. As a result, nodes with high CoI are more likely to engage with one another and establish a reliable bond. The computation of CoI-on the basis of trust in between 2 nodes is as follows:

$$T_{CoI}(i,j) = \frac{|C_i \cap C_j|}{C_i} \qquad (2)$$

where C_i and C_j stand in for the communities of nodes i and j, respectively.

3) Cooperativeness (CoP): Is a third factor that indicates how socially cooperative a trustee is with a trustor. We may use the entropy function described in [2] to work out CoP-based trust as:

$$T_{CoP}(i,j) = -T_p \log T_p - (1 - T_p)\log(1 - T_p) \qquad (3)$$

where T_p indicates the fraction of messages sent during the interaction because CoP is a measure of balance in the collaboration between the hubs.

4) Reward/Punishment: To keep up with both trustworthy relations and punish mischievous hubs, we utilize an outstanding downsizing recipe to give the motivation to legitimate hubs and punishments to misbehaving nodes as:

$$T_{Reward}(i,j) = \frac{|Int - Int_U|}{|Int|} e^{-\left(\frac{|Int_U|}{|Int|}\right)} \qquad (4)$$

Where Int_U denotes the count for the quantity of unproductive collaborations between hub I and hub j. Int_U features the total number of interactions.

As stated in Eq. (5), a linear equation with a weighting factor has traditionally been used to aggregate the overall trust; nevertheless, this method has many drawbacks and difficulties when deciding on the right weights.

$$T_{Direct}(i,j) = w_1 T_{FS}(i,j) + w_2 T_{CoI}(i,j) + w_3 T_{CoP}(i,j) + w_4 T_{Reward}(i,j) \qquad (5)$$

We therefore offer a novel machine learning-based technique that blends immediate and roundabout trust to decide general trust esteem in order to address this shortcoming. This method also determines how each of these characteristics affects the total trust value.

B. *Indirect Trust Measures (ITM)*

To decide the legal administrator or trustee in light of the assessments of different hubs in the organization, a indirect trust metric (ITM) is used. However, because nodes' eputations differ from one another, it is not ideal to consider every node in the network when calculating a trustee's reputation. As a result, in this study, nodes with at least one friend in common with both the trustor and the trustee are asked to provide reputation value. Finally, we create a method that is Algorithm 1 [2] to combine both indirect trust and direct trust to determine a single value of trust. The

aforementioned algorithm uses direct trust and suggestions as inputs and outputs a single trust value for each node, either trustworthy or untrustworthy. As can be seen, our trust score estimate technique relies more on direct trust. The node is neither trustworthy nor untrustworthy in this case, according to the neutral manifest. Furthermore, our approach does not automatically label the node as trustworthy if the direct trust is 0 or deceitful and the quantity of dependable proposals is more prominent than the quantity of dishonest suggestions, or (|T| > |U|). All things considered, a level of solid proposals (PT) is determined, and in the event that PT surpasses the limit (θ), in this model 70% or 0.7, the hub is assigned as dependable. The worth of θ totally relies upon the application, and for our situation the reasoning for the high worth of is to manage the issue of good mouthing and voting form stuffing assaults by giving the trustor hub more authority than the suggestions from different hubs in the organization. Similar to the previous method, this one executes when the direct trust is 1 or trustworthy.

When a node's trust score of direct is 2 or neutral, it means that recommendations are used to determine a node's trustworthiness rather than the trustor node having its own observations of the trustee. Node is labelled as trustworthy if |T| > |U|; else, it is untrustworthy.

Algorithm 1 Trust Score Estimation

$0 \rightarrow Untrustworthy, 1 \rightarrow Trustworthy, 2 \rightarrow Neutral$
Input: Direct Trust {0, 1 or 2}, Recommendations { $|T|$, $|U|$, and $|N|$ },
Output: Single Trust Score {0 or 1},
$|T| \rightarrow No: of\ Trustworthy\ Recommendations$,
$|U| \rightarrow No: of\ Untrustworthy\ Recommendations$,
$|N| \rightarrow No: of\ Neutral\ Recommendations$,
$\theta \rightarrow Threshold\ (\%)$,
$P_U \rightarrow Untrustworthy\ Recommendations\ (\%)$,
$P_T \rightarrow Trustworthy\ Recommendations\ (\%)$
if There are no Recommendations **then**
  $Final\ Trust = Direct\ Trust$
end if
if $Direct\ Trust == 0$ **then**
  if ($|U| >= |T|$ || ($|N| >= |T|$ && $|N| >= |U|$) **then**
    Node is Untrustworthy
  else
    $P_T = \frac{|T|}{Total\ Recommendations+1}$
    if $P_T >= \theta$ **then**
      $Node\ is$ **Trustworthy**
    else
      $Node\ is$ **Untrustworthy**
    end if
  end if
else if $Direct\ Trust == 1$ **then**
  if ($|T| >= |U|$) || ($|N| >= |T|$ && $|N| >= |U|$) **then**
    Node is Trustworthy
  else
    $P_U = \frac{|U|}{Total\ Recommendations+1}$
    if $P_U >= \theta$ **then**
      $Node\ is$ **Untrustworthy**
    else
      $Node\ is$ **Trustworthy**
    end if
  end if
else
  if ($|T| > |U|$) **then**
    $Node\ is$ **Trustworthy**
  else
    $Node\ is$ **Untrustworthy**
  end if
end if

IV. Analysis And Findings

To categorise the associations as trustworthy or untrustworthy, k-means clustering was used. But rather than classifying the material into just two groups, the elbow technique divides it into three groups: neutral, untrustworthy, and trustworthy. Since it is not possible to view all of the features at once, we did not use all of the characteristics for clustering in the demonstration, only the pairs of trust features. However, we may determine the outcomes for simultaneously viewing all of the characteristics by using the analysis of principle component has procedure for aspect decrease, for instance, from five to three for our situation [9]. By contrasting F S and CoI and F S with Remuneration, individually, the dispersion of trust values shows that the locales with CoI>= 0.5 and Prize >= 0.5 are dependable, while the districts with CoI = 0.3 and Award = 0.3 are deceitful. As trust esteem for the most part relies upon CoI and Prize, it exhibits an unmistakable predominance of CoI and Compensation on F S.

After the labels have been successfully investigated, the following stage is to prepare our model to decide if the cutting-edge connections of SIoT hubs are dependable. Following the execution of a regulated learning calculation (irregular backwoods), the choice limit accurately and precisely sorts the hubs. Obviously, our model has generally important capacities for arranging modern collaborations as nonpartisan, dependable, or dishonest. Fig. 3 shows the significance (i.e., weightage) of every not entirely set in stone subsequent to applying our model to the dataset and the classification algorithm's accuracy (99.1%).

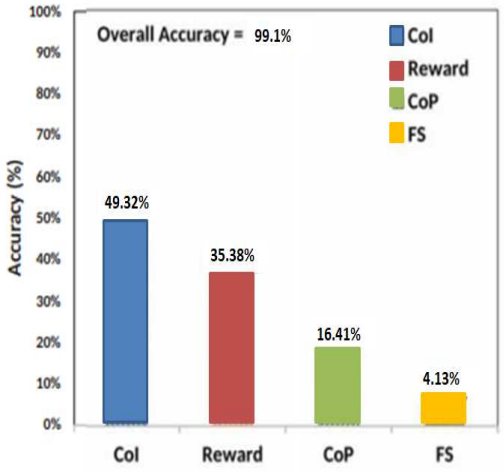

Figure 3: Accuracy of Model and Weightage of Feature.

It is clear that CoP (16.41%) and F S (4.13%) have less of an impact on the total trust score than CoI (49.32%) and Reward (35.38%) do. The main justification for the increased weight placed on CoI is that objects that belong to the same group tend to be more reliable and engage in more regular interaction. Similar to the previous example, the feature of Reward shows that more fruitless connections increment dishonesty, making it an essential part in deciding the trust score.

Despite the fact that we have grouped nodes into three classes — trustworthy, untrustworthy, and neutral as a rule, simply have to classify a hub as dependable or dishonest. Subsequently, the size of the groups was diminished to two to

be pragmatic for genuine applications. If and when there is an irreconcilable circumstance between the trustor and different hubs in the organization, we combined the trust score using a percentage threshold (). For example, if direct trust = trustworthy and there are more unreliable suggestions (|U|) than reliable recommendations (|T|), our method looks into the proportion of unreliable recommendations (PU). The node is labelled as untrustworthy if PU >.

We compared several thresholds to determine the ideal value of, and when = 70%, as shown in Fig. 4, our algorithm exhibits the highest accuracy of 90.1%. But when direct and indirect trust is combined, our algorithm's accuracy is a little bit lower than the model's accuracyat the point when just direct trust is considered. This is generally brought about by the shortfall of any earlier cooperations between the hubs, which at first prompted more noteworthy trust levels. Subsequently, suggestions are continually used to decide the substantial outcomes, which bring down the exactness generally, in order to avoid such situations.

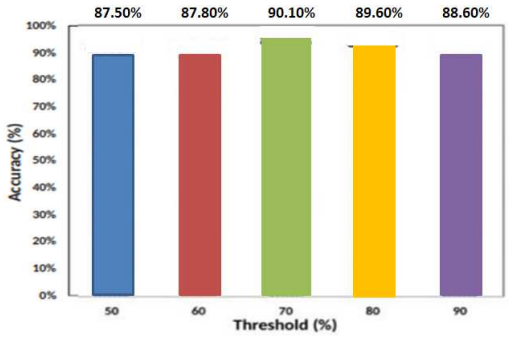

Figure 4: Accuracy of Trust Estimation

V. CONCLUSION

As opposed to the ordinary weighted heuristics, we have introduced an ML based trust management strategy in this research to determine a single score of trust for every SIoT node. In order to excerpt important trust aspects with regard to the SIoT domain, a trust management model has been imagined. The data is then classified utilizing k-implies bunching to decide the untrustworthy and trustworthy encounters in order to composite the trust. A trust prediction technique has also been put forth to help determine decision thresholds and to understand how different variables affect the overall trust score. Our results show further developed exactness in distinguishing dependable collaborations.

We want to add knowledge as a trust characteristic for the computing of indirect and direct trust in the near future in order to compile the target nodes' prior interaction history together with a few other social traits, such as social relationships in regards to co-work and co-location. This might lead to a more accurate identification of reliable SIoT network nodes.

REFERENCES

[1] Yang, H., Zhong, W. D., Chen, C., Alphones, A., & Xie, X. (2020). Deep-reinforcement-learning-based energy-efficient resource management for social and cognitive internet of things. *ieee internet of things journal*, *7*(6), 5677-5689. https://doi.org/ 10.1109/JIOT.2020.2980586

[2] Sagar, S., Mahmood, A., Sheng, Q. Z., & Zhang, W. E. (2020, June). Trust computational heuristic for social Internet of Things: A machine learning-based approach. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICC40277.2020.9148767

[3] Khan, W. Z., Hakak, S., & Khan, M. K. (2020). Trust management in social internet of things: Architectures, recent advancements, and future challenges. *IEEE Internet of Things Journal*, *8*(10), 7768-7788. https://doi.org/10.1109/JIOT.2020.3039296

[4] Caminha, J., Perkusich, A., & Perkusich, M. (2018). A smart trust management method to detect on-off attacks in the internet of things. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/6063456

[5] Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering*, *81*, 106522. https://doi.org/10.1016/j.compeleceng.2019.106522

[6] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1761-1804. https://doi.org/10.1109/COMST.2020.2997475

[7] Jaasinghe, U., Lee, G. M., Um, T. W., & Shi, Q. (2018). Machine learning based trust computational model for IoT services. *IEEE Transactions on Sustainable Computing*, *4*(1), 39-52. http://doi.org/10.1109/TSUSC.2018.2839623

[8] Truong, N. B., Lee, H., Askwith, B., & Lee, G. M. (2017). Toward a trust evaluation mechanism in the social internet of things. *Sensors*, *17*(6), 1346. https://doi.org/10.3390/s17061346

[9] Shlens, J. (2014). A tutorial on principal component analysis. *arXiv preprint arXiv:1404.1100*. https://doi.org/10.48550/arXiv.1404.1100

[10] 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: Proceedings, https://Doi.Org/10.1016/J.Matpr.2021.03.642

[11] A. Jain, A. K. Pandey, (2019),"Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191. https://doi.org/10.1016/j.matpr.2019.06.292

[12] 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. https://doi.org/10.1016/j.matpr.2019.12.010

[13] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261. https://doi.org/10.1016/j.matpr.2017.07.054

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