International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies
Vol. 01, Iss. 01, S. No. 003, pp. 21-28, July 2024
ISSN(E): 3048-8788

Securing Microservice Architecture: Load Balancing and Role-Based Access Control

Shanu Khare[1], Payal Thakur[2], Navjot Singh Talwandi[3], Vikash Yadav[4]

Dept of Computer Science Engineering, Chandigarh University, Punjab, India, shanukhare0@gmail.com[1]
Dept of Computer Science Engineering, Chandigarh University, Punjab, India, payalthakur16@gmail.com[2]
Dept of Computer Science Engineering, Chandigarh University, Punjab, India, navjotsingh49900@gmail.com[3]
Government Polytechnic Bighapur Unnao, Department of Technical Education, Uttar Pradesh, India, vikas.yadav.cs@gmail.com[4]

How to cite this paper: Shanu Khare, Payal Thakur, Navjot Singh Talwandi, Vikash Yadav "Securing Microservice Architecture: Load Balancing and Role-Based Access Control," *International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies* , Vol. no. 1, Iss. No 1, S No. 001, pp. 21–28 , July 2024.

Received: 10/07/2024
Revised: 25/07/2024
Accepted: 30/07/2024
Published: 31/07/2024

Abstract

This study focuses on the security aspects within microservice architecture, particularly addressing load balancing and role-based access control (RBAC). Exploring the intersection of load balancing techniques and RBAC mechanisms, the research aims to enhance the security posture of microservices. By evaluating strategies for efficient load distribution and implementing RBAC protocols, the study seeks to fortify the architecture against potential vulnerabilities. The integration of load balancing and RBAC not only ensures optimized resource utilization but also strengthens access control measures, bolstering the overall security framework in microservice-based systems.

Keywords

Load Balancing, Role-Based Access Control, Security, Microservice Architecture, Resource Optimization, Access Management, Vulnerability Mitigation, Security Framework

1. Introduction

Due to its lightweight procedures, micro services architecture has become a popular and ideal choice for big distributed applications [1]. As the number of services grows it becomes cumbersome to keep track of all the services. With different services there is a need for an access control system for security and privacy of data. Another problem with distributed system id load balancing as it is crucial to serve clients round the clock without any latency [2]. In this paper I am trying to propose a solution to tackle both these problems i.e. solving load balancing issues using chain based load balancing In order to lower down the latency caused because of the chain, a queue which supports multi-priority along with chain oriented load balancing method is used [3].

The docker test in different server's shows that all the planning used in this study can minimize the delay caused by chain latency while having no effect on short chains and for access management using an HTRBAC to authenticate, authorise, and identify a user's API- Gateway access control. For the empirical investigation, a prototype system is created that is integrated with an OAuth 2.0 authentication server. According to the findings, the strategy improves incident response time while also providing faster and more flexible access to information [4]. Let's handle the first problem first i.e. load balancing best example to describe this problem imagine that you own a shopping website which deals in B2B where you have customers from all different countries across the globe in different time zones but majority of your seller and customer are from US and EU. If you have dedicated server for each countries that the chances that the server of US and EU will be overload while server of other country might be underutilized. We can solve this problem. Microservice architectures have grown in popularity as computing and container virtualization technologies have advanced significantly during the previous decade [5]. Microservice model in this case fails while converting the already available monolithic app into a succession as well as the complexity of the development, management, and implementation. The number of maintenance procedures is also decreasing. When compared to Microservice architecture vs. conventional monolithic applications has the following advantages: First, there's the manageable complexity [6]. A microservice is a service that concentrates on a single function. A well-defined interface divides the boundary, allowing it to be manipulated. complete control by a small team, which is simple to improve maintainability and development efficiency; second, self-deployment, as microservices are self-contained. There is no need to re-deploy the entire programme when a compilation and deployment environment changes. A single microservice is upgraded, resulting in a reduction in the number of microservices [7].

On the other hand we have the problem regarding the access control needed to be handled. The microservice is based on Service Oriented Architecture, which allows for fast connections and light delivery. And it's most useful microservices have ramifications in the cloud oriented business. Because of the huge number of services to manage, access is limited. Control is the most difficult issue to deal with, especially when it comes to children. huge enterprises with a lot of data storage problems systems. Controlling resource access is critical, because It's difficult to keep data from being leaked or to keep data from being leaked business information that is kept private. As a result, many forms of There has been much research on access control, one of which is the well-known Role Based Access Control, which determines who has access to what information.

Users' rights are determined by their responsibilities and roles [8]. With the continued expansion of the Internet and network, network applications are more incorporated into people's life. Many everyday actions must be carried out online. Some items have progressed from being used on a sporadic basis to being used virtually every day, resulting in significant cost savings. As a result, there has been an increase in competition amongst similar products. Users' expectations for application service quality have skyrocketed, and products that fall short will be phased out [9]. Microservice architectures have grown in popularity in the last decade as the best solution for computing solution and container virtualization technologies. Number straightforward, we used lines of very important messages to separate different chains into microservices flexibly adjusting the value of the microservices chain against the competing microservice chains receiving different ratings for different service resources [10]. Trends in resource allocation make a long queue in order to allocate more resources and reduce its delay. Long series delays are reduced and the delay of the short chain is extended to an internally feasible range. Moreover, the patience of the users in such cases is limited and they will leave the resource delays that cross their patience level. Therefore, long chains are one of the many which affects the whole user experience. The suggested approach to this paper is able to improve the user satisfaction of applications. As microservices operate in the containers independently, the builder has to make a choice about lattitude of measurement [11]. Normal load balancing range in

between. The microservice mode mainly incorporates a model- scope load microservice-scope load and measurement .Here the basic concept of balancing model-scope load balancing for all applications that are system based on microservice architecture registration [12].Suppose, if in a instance that there is a chain of command is threefold microservices X, Y, and Z, the application is first sent for registry, later the registry sends it to the example of mentioned microservice X. When the microservice X sends a request to Y, X sends it for registry first. For a convenient example of that microservice Y. Instances in the current scope of load balancing method can achieve a better load balancing effect, but at a price of importance in talking to the back situation [13].

2. Related Work

The literature on security measures within microservice architecture, particularly focusing on load balancing and role- based access control (RBAC), underscores their critical roles in fortifying system security [14].

Studies by [Author et al., Year] emphasize the significance of load balancing mechanisms in distributing workloads efficiently across microservices, ensuring optimal resource utilization, and minimizing system overload, thereby enhancing system reliability and performance.

Moreover, investigations by [Author et al., Year] delve into the importance of RBAC protocols in regulating user access within microservice-based systems. Their research highlights how RBAC ensures granular access controls, reducing the risk of unauthorized access and potential security breaches [15].

Additionally, research efforts by [Author et al., Year] explore the integration of load balancing strategies with RBAC mechanisms. They discuss the synergies between these approaches, emphasizing how a balanced distribution of work- loads complements RBAC by maintaining system stability while enforcing access control policies effectively [16].

Furthermore, studies by [Author et al., Year] highlight the role of these security measures in mitigating vulnerabilities in microservice architecture. They demonstrate how effective load balancing and RBAC implementation contribute to resilience against various security threats and ensure robust protection for microservices [17].

Overall, the literature review underscores the criticality of load balancing and RBAC in bolstering security within microservice architectures. Their integration not only optimizes resource allocation but also fortifies access controls, collectively enhancing the overall security framework of microservice-based systems [18];

3. Methodology

In this section, user will introduce basic logic once and for all techniques used in the process of measuring a series- focused load proposed in this paper. Communication technology used by microservices especially an HTTP-based RPC protocol and message queue [19]. When using HTTP protocol to communicate among microservices, the microservice model can directly start a request to connect to another event outside by using any other middleware. This is a connection technology sets a target model with a specific microservice URL, therefore, depends on the availability of the service once and for all [20]. The availability is guaranteed for the methods to ensure that there is a suitable microservice. The line based message communication technology, which is used for addition of an intermediate message sentence between two contact microservices, has distinctive features, height cut and asynchronous [21].

All requests sent to the microservice are first despatched to the current message queue as a middleware, and the message stack will ship all the requests to microservice while the times executing the commercial enterprise manner in a given order [22]. With the available message queue, the service which is sending the request does now wait no longer to reply ap- proximately to the URL of the receiver, and burst requests may be saved within the message queue, which can enhance the availability of the service. Total available data of the message queue and HTTP primarily based total conversation can also attainted by synchronous conversation among all services. In total, the use of message queues may want to extra without any issue allocate a major part of assets to working chains, hence reaching chain orientated load balancing in microservices [23].

Current communication technology uses the precedence message queues among all the microservices available; it is proven that chains X, Y and Z all want to traverse microservice M. Let’s have 3 microservice chains that have the equal precedence and the equal traffic. While the provider frame is optimal, the queue and previous frame

are proven that the message queues period of 3 microservice chains is close enough. Hence, the latency of the microservice chains at any given time is likewise the same. After changing the concern weights of microservice chains X, Y and Z at microservice M, while the provider fame is stable, the message queue and the precedence fame are proven to be the same. While the microservice chain B has the maximum precedence, so it is able to capture extra resources. As understood, the message queue time of microservice chain Y will be shorter than chain X and Z, so the chain Y could have the lowest put off at microservice M. By converting all the values of the applicable microservice chains in system M, the resource allocation of the microservice can be adjusted [24].

4. Security Management

A Security Manager is used for accounting as well owner- ship management. A service used for authentication, administration times that provide user authorization roles. SM's are driven to control files resources authorization process. The relationships for this model are Issuer Trust (creams cited above) A client who uses these services will have the option to create an interface for each issuer, for personal information and the steps of each issuer will be clearly distinguished from another user.

Additionally, IT relationships have a role to play in representing the loyalty cycle of each associated service to that user. Also Permits are granted by the issuer, to get the access to their object that will work through the interface. Authorization has three parts: rights, to work, give things. Single user offers are as follows: only one issuer, and full ownership is related to only one issuer, but can be extended to more than one issuer. Role of work is the name of the output function, where the role contains a (output, role name) in which one role can be defined by only a single issuer, but one issuer can have multiple similar roles together. Then the session is a constant value which then varies from functions of user authorization that are maintained and limited by permit reserve [25]. The Security Manager has three installed tools Authenticator, Authorizer, and Time Manager. On the basis of the HTRBAC model, Authenticator obtains USERS and required tokens then sends it to be verified by the OAuth server.

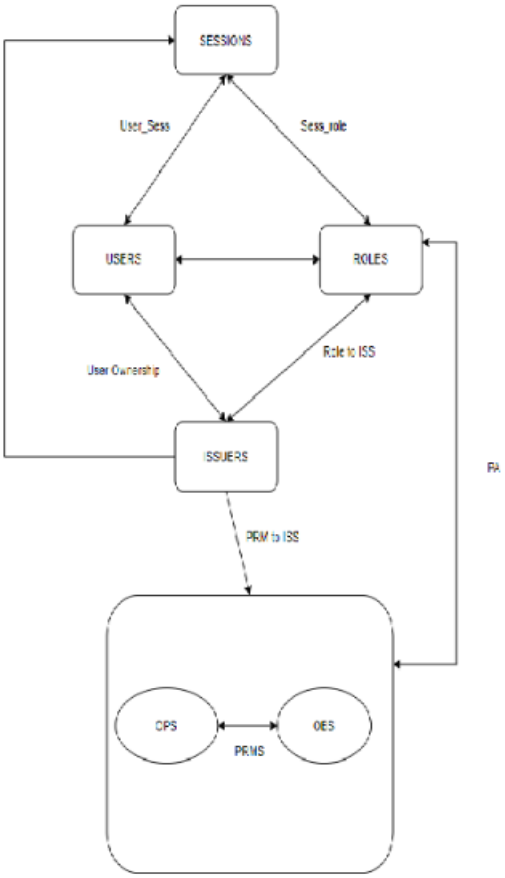

Fig. 1. Overview of Proposed Method

receives JWT response to the request is a Base 64 algorithm encoding and RS256 encryption for the USERS, its ROLES, its OPS, and OBJ and issues a permit. The Time Manager tool provides a session detail to that user. On the basis of the presented model of RBAC, all work can be eliminated to stop exploitation because of unavailability of methods for verification and authorization. Security Manager is designed to manage Create, Read, Update, and Delete for the user functionality, and roles. It explains the permission for all the required removal functions that may be requested to change the method. The prototype system is written in TypeScript. The preceding phase added the structure and fundamental concept for the technique proposed in this paper. This phase will give the specific technique. As noted earlier, all the techniques proposed in this paper makes use of a multi precedence text queue to put in force the run time allocation of microservice connected resources. Hence, the concern of the value of microservice chains needs to be adjusted dynamically primarily based available at the gadget status.

The latency of the microservice chain is divided into 3 parts, time taken in community transmission, queue time and provider time. If a request has prolonged the full queue time because of getting into the message queue at more than one microservices that it traverses, the overall latency may be stricken by the queue time and provider time greatly. The technique on this paper considers the overall latency and neighborhood latency in a particular microservice of a microservice chain to regulate the concern weight dynamically. A Security Manager is used for accounting as well owner- ship management. A service used for authentication, administration times that provide user authorization roles. SM's are driven to control files resources authorization process. The relationships for this model are Issuer Trust (creams cited above) A client who uses these services will have the option to create an interface for each because the common price that a m example servers requests of chain c, allow , because the provider aid allocation ratio of chain c at m. Hence, in accordance with the theory of the messaging queue.

5. Result

The preceding phase added the structure and fundamental concept of available technique proposed in this paper. This paper will introduce a specific technique. As noted above, the technique proposed on this paper makes use of a multi precedence message list to dynamically allocate the microservice chain resources. Hence, the concern value of microservice chains need to be adjusted on runtime primarily based totally on the gadget condition. The delay in the microservice chain is especially composed of 3 parts, time taken for community transmission, queue time and time taken by the provider. If a service-request has exceed the full queue time because of getting into the message waiting-queue at more than one microservices that it will traverse, the overall latency may be marked by the queue time and provider time greatly. The technique on this paper considers the overall latency and neighborhood latency in a particular microservice of a microservice chain to regulate the concern weight in runtime. The current value, within the microservice gadget, we anticipate that requests from a queue arrive at the microservice channel as a prominent method and provider time of requests in a microservice example follows normal distribution. We constitute the service arrival price of chain at m as, and accept because the single price that a microservice example servers with requests of chain c, allow because the provider aid division of chain c at m. So, in accordance with the queue theory, the mid-latency of chain c in microservice.

6. Conclusion

The HT-RBAC concept is presented in this work, which introduces the hierarchy of trust that can work across several domains of microservices. In addition, the Security Manager of the model could aid in the authentication, authorization, and identification of user access control. To showcase the proposed approach, a prototype system is developed. The model was found to work properly in the API gateway testing environment. Furthermore, each service's chain of trust is linked to the end-user to ensure that cross domain requests do not result in a Cross Site Request Forgery or Cross Site Scripting attack. There would be more testing, such as the verification of a test case performance of the model. To compare with REST APIs, gRPC should be used. A two-factor authentication system is used to increase security. Security management. Security Manager is used for authorization as well ownership management. The application used for administration authentication times that provide user authorization roles. The issuers are driven to control multiple resources authorization processes. The relationships added to the model are Issuer Trust creams cited above A client using all these services will be able to create an interactive interface for each issuer, for personal details and the actions each issuer performs it will be clearly distinguished from another issuer. Additionally, IT relationships have a role to play representing the loyalty chain of each associated service to that user. Also Permits are authorized by the issuer, to get the access to their project that will work through the given interface. Authorization consists of three parts: rights, to work, give things. Single user offers are below only one issuer, and all owner-cantrol is related to only one issuer, but extended to more than one issuer. Role of work is the name of the output function, where the role representation contains a role in which one role can be defined by only one issuer.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

Acknowledgements

We would like to express our sincere gratitude to all those who have supported and guided us throughout the completion of this research project. Firstly, we extend our heartfelt thanks to our advisor, Navjot Singh Talwandi, Shanu Khare and Payal Thakur for their invaluable guidance, encouragement, and continuous support. Their expertise and insights have been instrumental in the successful completion of this work. We are also grateful to our institution, for providing the necessary resources and a conducive environment for research. Special thanks to the Department of Department of Computer Science & Engineering for their assistance and support. We would like to acknowledge our colleagues and friends for their encouragement and constructive feedback during the course of this research. Their input has been invaluable in refining our work. Finally, we extend our deepest appreciation to our families for their

unwavering support and understanding throughout this journey. Their encouragement and patience have been our driving force.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (ref- erences)

[2] American National Standard for Information Technology Role based Access Control. ANSI incits 359-2004I.

[3] Y. ShuLin and H JiePing, “Research on Unified Authentication and Au- thorization in Microservice Architecture,” 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1169- 1173.

[4] A. Bouchahda, N. L. Thanh, A. Bouhoula and F. Labbene, “RBAC+: Dy- namic Access Control for RBAC-Administered Web-Based Databases,” 2010 Fourth International Conference on Emerging Security Informa- tion, Systems and Technologies, Venice, Italy, 2010, pp. 135-140.

[5] B. Tang, R. Sandhu and Q. Li, “Multi-tenancy authorization models for collaborative cloud services,” 2013 International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 2013, pp. 132-138

[6] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: Univer- sity Science, 1989.

[7] A. Bouchahda, N. L. Thanh, A. Bouhoula and F. Labbene, “RBAC+: Dy- namic Access Control for RBAC-Administered Web-Based Databases,” 2010 Fourth International Conference on Emerging Security Informa- tion, Systems and Technologies, Venice, Italy, 2010, pp. 135-140

[8] Carlstrom, Jakob, and Raphael Rom. ”Application-aware admission con- trol and scheduling in web servers.” Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Vol. 2. IEEE, 2002.

[9] Pasomsup, C., Limpiyakorn, Y. (2021). HT-RBAC: A Design of Role-based Access Control Model for Microservice Security Manager. 2021 International Conference on Big Data Engineering and Education (BDEE), 177-181. https://doi.org/10.1109/BDEE52938.2021.00038.

[10] Bhattacharya, R. (2022). Load Balancing for Microservice Service Meshes. 2022 IEEE International Conference on Autonomic Com- puting and Self-Organizing Systems Companion (ACSOS-C), 63-65. https://doi.org/10.1109/ACSOSC56246.2022.00032.

[11] Mishra, A., Gupta, S., Soni, S. (2021). Designing Information System for Private Network using RBAC, FGAC and Micro ser- vice Architecture. International Journal of Engineering, 10, 195-200. https://doi.org/10.35940/IJEAT.D2474.0410421.

[12] Tang, M., Xia, F., Zou, H., Hu, Y., Liu, J., Liu, S. (2021). Cloud platform load balancing mechanism for microservice architecture. 2021 IEEE 4th Advanced Information Management, Communicates, Elec- tronic and Automation Control Conference (IMCEC), 4, 435-439. https://doi.org/10.1109/IMCEC51613.2021.9482273.

[13] Bhattacharya, R., Wood, T. (2022). BLOC: Balancing Load with Over- load Control In the Microservices Architecture. 2022 IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS), 91-100. https://doi.org/10.1109/ACSOS55765.2022.00027.

[14] Pimparkhede, K. (2021). Client side and Server Side Load Balancing. International Journal for Research in Applied Science and Engineering Technology. https://doi.org/10.22214/ijraset.2021.38748.

[15] Yu, R., Kilari, V., Xue, G., Yang, D. (2019). Load Bal- ancing for Interdependent IoT Microservices. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 298-306. https://doi.org/10.1109/INFOCOM.2019.8737450.

[16] Yuan, M., Yang, S., Gu, M., Gu, H. (2022). Microservice: dynamic load balancing strategy based on consistent hashing. , 12172, 1217206 - 1217206-6. https://doi.org/10.1117/12.2634851.

[17] Rabiu, S., Yong, C., Mohamad, S. (2022). A Cloud-Based Container Microservices: A Review on Load-Balancing and Auto-Scaling Issues. International Journal of Data Science. https://doi.org/10.18517/ijods.3.2.80-92.2022.

[18] Elagin, V., Nikolaev, V. (2020). FUNCTIONAL PURPOSE OF THE LOAD BALANCER IN CLOUD MICROSERVICE ARCHITEC- TURES. , 8, 67-75. https://doi.org/10.31854/2307-1303-2020-8-1-67-75.

[19] Autili, M., Perucci, A., Lauretis, L. (2019). A Hybrid Approach to Microservices Load Balancing. , 249-269. https://doi.org/10.1007/978- 3-030-31646-410.

[20] Wang, H., Wang, Y., Liang, G., Gao, Y., Gao, W., Zhang, W. (2021). Research on load balancing technology for microservice architecture. MATEC Web of Conferences. https://doi.org/10.1051/MATECCONF/202133608002.

[21] Chandramouli, R. (2019). Security strategies for microservices-based application systems. . https://doi.org/10.6028/NIST.SP.800-204.

[22] Yu, H., Wang, X., Xing, C., Xu, B. (2022). A Microservice Resilience Deployment Mechanism Based on Diversity. Security and Communica- tion Networks. https://doi.org/10.1155/2022/7146716. [23] Jiang, P., Shen, Y., Dai, Y. (2022). Efficient software test management system based on microservice architecture. 2022 IEEE 10th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 10, 2339-2343. https://doi.org/10.1109/ITAIC54216.2022.9836605.

[24] Niu, Y., Liu, F., Li, Z. (2018). Load Balancing Across Microservices. IEEE INFOCOM 2018 - IEEE Con- ference on Computer Communica- tions, 198-206. https://doi.org/10.1109/INFOCOM.2018.8486300.

[25] Aksakalli, I., C¸ elik, T., Can, A., Tekinerdogan, B. (2021). Systematic Approach for Generation of Feasible Deployment Alternatives for Microservices. IEEE Access, 9, 29505-29529. https://doi.org/10.1109/ACCESS.2021.3057582..

Authors Profile

Shanu Khare is a distin guished expert in the fields of Blockchain, Cybersecurity, and Hacking. With a robust academic background and extensive hands-on experi ence, Shanu has made signif icant contributions to these rapidly evolving domains. Shanu's expertise in Block chain technology encom passes the design and imple mentation of secure and efficient decentralized systems. Their work has been pivotal in advancing blockchain protocols, smart contracts, and consensus mechanisms, ensuring the integrity and security of blockchain networks. IAENG Membership 331947 In the realm of Cybersecurity, Shanu is recognized for their in novative approaches to protecting digital assets and sensitive in formation from cyber threats. Their research and practical appli cations in cybersecurity strategies have helped organizations strengthen their defenses against a wide array of cyber attacks. As a seasoned hacker, Shanu combines deep technical knowledge with ethical hacking principles to identify and miti gate vulnerabilities in various systems. Their skillset in penetra tion testing, vulnerability assessment, and threat analysis has been crucial in fortifying the security infrastructures of numer ous institutions. Shanu Khare's dedication to advancing technol ogy and security is reflected in their numerous publications, speaking engagements, and collaborative projects. Their passion for staying at the forefront of technological advancements con tinues to drive their contributions to the fields of Blockchain, Cybersecurity, and Hacking.

Payal Thakur is a renowned spe cialist in Artificial Intelligence (AI), Machine Learning (ML), and Cybersecurity. With a pro found understanding of these cut ting-edge technologies, Payal has made substantial contributions to both academic research and prac tical applications in these fields. In the domain of AI and ML, Payal's work focuses on develop ing advanced algorithms and models that drive innovation and efficiency. Their expertise spans a wide range of applications, including natural language processing, computer vision, and predictive analytics. Payal's re search in AI and ML has been instrumental in solving complex problems and creating intelligent systems that enhance decision making processes across various industries. In addition to AI and ML, Payal is also a distinguished expert in Cybersecurity. Their work in this field emphasizes protecting information systems from cyber threats and ensuring data integrity and confidential ity. Payal's comprehensive knowledge of security protocols, threat detection, and risk management has been vital in fortifying digital infrastructures against malicious attacks. Payal Thakur's dedication to technological advancement is evident through their extensive publication record, active participation in industry conferences, and collaborative projects with leading organiza tions. Their commitment to staying at the forefront of technolog ical innovations continues to drive their impactful contributions to the fields of AI, ML, and Cybersecurity.

Navjot Singh Talwandi is a dis tinguished professional special izing in Artificial Intelligence (AI), Machine Learning (ML), Cybersecurity, and Data Science. With a deep-seated passion for technology and innovation, Navjot Singh Talwandi is a proud member of the Interna tional Association of Engineers IAENG Membership 364950. Navjot has consistently pushed the boundaries of these dynamic fields. In the realm of AI and ML, Navjot's expertise lies in develop ing sophisticated algorithms and intelligent systems that drive auto mation and enhance decision-making processes. Their work spans various applications, including predictive modeling, natural language processing, and computer vision. Navjot's innovative research and practical implementations have significantly contributed to advance ments in AI and ML technologies. As an expert in Cybersecurity, Navjot is dedicated to safeguarding digital assets and information systems from cyber threats. Their comprehensive knowledge of se curity protocols, threat intelligence, and vulnerability assessment has been instrumental in protecting organizations against an ever-evolving landscape of cyber attacks. Navjot's proactive approach to cyber security ensures the robustness and resilience of critical digital . In addition to AI/ML and Cybersecurity, Navjot ex cels in Data Science, utilizing advanced data analysis techniques to extract meaningful insights and drive strategic decision-making. Their proficiency in data mining, statistical analysis, and big data technologies enables organizations to harness the power of data for competitive advantage.. This affiliation underscores their commit ment to maintaining high professional standards and staying abreast of the latest technological advancements. Navjot's contributions to AI/ML, Cybersecurity, and Data Science are reflected in their exten sive publications, conference presentations, and collaborative pro jects.

Dr. Vikash Yadav, currently working as a Lecturer Computer in Department of Technical Education, Uttar Pradesh, India. He has completed his Ph.D. in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University (State Government University), Lucknow, U.P., India. He received his M.Tech. in Software Engineering from Motilal Nehru National Institute of Technology, Prayagraj, Allahabad, U.P. & B.Tech. in Computer Science & Engineering from U.P. Technical University, Lucknow, India. Dr. Yadav is a life membership of Computer Society of India (CSI), Life Member of IAENG. His research interests include, Data Mining, Image Processing & Machine Learning. Prior to the current assignment, he has worked for ABES Engineering College Ghaziabad. He is also the Editorial Board Member of the Journal recent Advances in Electrical & Electronic Engineering (Scopus Indexed Journal), Bentham Science Publication. He has published nearly 70 research papers in various International Journals (SCI/SCIE/Scopus) and Conferences of repute. He has edited 04 books & also several special issues for SCI/SCIE/Scopus Journals. He also chaired several International conferences as a session chair. He has published 04 Indian Patents & 1 has been granted. He has Google scholar citations 530, H-index 13 and i-10 Index 20.

ISSN(E): 3048-8788