rice2024 Proceedings of the Ninth International Conference on Research in Intelligent Computing in Engineering pp. 151–155
DOI: 10.15439/2024R75
ISSN 2300-5963 ACSIS, Vol. 42

Real Time Adaptive Access Control with Behavioral Analytics for Enhanced Cybersecurity in IoT and Cloud Systems

Abhishek Tripathi
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
tripathi.abhishek.5@gmail.com

Kumar Rajan
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
99210041069@klu.ac.in

Vishwajit Kumar
Department of Computer Science and Engineering
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
99210041302@klu.ac.in

Kumar Raj
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
99210041068@klu.ac.in

V Prasanna Anajaneyulu
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
99210041813@klu.ac.in

Atul Sharma
Malaviya National Institute of Technology,
Jaipur, Rajasthan, India
atul.mrc@mnit.ac.in

Thangamani Ramesh
Kalasalingam Academy of Research and Education
Srivilliputhur, Tamil Nadu, India
ramesh.ramesh81@gmail.com

Pooja Bhamre
Sardar Vallabhbhai National Institute of Technology
Surat, Gujarat, India
poojamkhairnar@gmail.com

***Abstract*—DACS dynamically adjusts access permissions by analyzing user behavior, context, and risk in real time. It evaluates activity logs, device details, and network conditions to identify anomalies, such as irregular login times or unfamiliar devices, triggering access restrictions or additional authentication. Using a neural network trained on historical data, DACS assigns risk scores to access attempts, categorizing them as low, moderate, or high-risk. Low-risk behaviors allow seamless access, while high-risk attempts undergo scrutiny. Our implementation demonstrates DACS's scalability, low latency, and superior detection accuracy compared to static models. These findings position DACS as a proactive, intelligent solution to address the dynamic challenges of secure access in real-time, high-demand environments.**

***Index Terms*—Access, Security, Behavior, Adaptation and Risk.**

I. Introduction

TRADITIONAL access control methods, based on fixed roles and rules, struggle to secure today's dynamic digital environments against sophisticated threats. Their static nature limits flexibility in adapting to changing user behavior and emerging risks, making systems vulnerable to unauthorized access. Dynamic Access Control Systems (DACS) address this by integrating real-time behavioral analytics to enable adaptive, context-aware security decisions. DACS continuously monitor user activity, assessing factors like location, device, and access time, and establish a baseline for typical behavior. Deviations trigger immediate adjustments to access permissions, responding intelligently to potential threats. This adaptive approach strengthens security by adding a nuanced, responsive layer of analysis, distinguishing DACS from traditional models. This study explores the design, algorithms, and security advantages of DACS, demonstrating its potential to provide robust and responsive security in today's evolving cybersecurity landscape, where static models like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) often fall short. The DACS address the limitations of traditional static access models by adapting permissions in real time based on user behavior, context, and risk [1, 2]. In smart home IoT, access control is especially challenging due to diverse devices and protocols, making systems vulnerable to emerging threats [2]. Traditional models like RBAC and ABAC are widely used but often lack the flexibility to manage dynamic environments effectively. Hybrid models combining RBAC and ABAC, such as HABACα and EGRBAC, have shown promise in providing fine-grained, context-aware access [1, 3].

These hybrid systems enhance security by integrating advanced authentication, like biometrics, to increase control precision [3]. By incorporating real-time risk assessment, DACS offer responsive, adaptive protection suited to modern interconnected systems. This paper examines DACS design and algorithmic structure, showcasing their potential to strengthen security in dynamic, IoT-driven environments [4, 5, 6].

Section II reviews access control mechanisms, Section III outlines the framework, Section IV details implementation,

Section V analyzes performance, and Section VI concludes with scalability and security insights.

II. Literature Review

In response, researchers are integrating elements from both RBAC and ABAC to develop hybrid access control models, leveraging the strengths of each. This integration yields a more granular control over access permissions by considering contextual factors, such as device type, location, and time, allowing for a dynamic response tailored to specific scenarios. For instance, in IoT environments, access control models like HyBAC integrate role- and attribute-based strategies to address smart home security challenges, adapting permissions based on the context and roles assigned to each device. Emerging technologies like machine learning, fog computing, edge computing, and blockchain further support the evolution of DACS by enhancing security in complex systems such as the Internet of Things (IoT). These technologies enable a more intelligent analysis of user actions and environmental conditions, allowing systems to adjust permissions dynamically in response to new threats. In this paper, we explore how DACS leverage behavioral analytics and risk assessment to achieve a flexible, context-aware security framework. This approach not only bolsters security by mitigating unauthorized access but also aligns access control with the nuanced demands of modern cybersecurity, ensuring data integrity in increasingly complex digital ecosystems.

The field of access control has evolved significantly, with recent advancements focusing on dynamic, adaptive models that enhance security in IoT, cloud, and distributed computing environments. Kim et al. [7] introduced an ABAC-based security model for Data Distribution Service (DDS), facilitating secure and dynamic data communication in distributed environments like healthcare by basing access on message content rather than participant identity. Addressing cloud security, Vijayanand and Saravanan [8] proposed the SACS-DACS system, which combines anomaly detection with dynamic access control to secure cloud servers. This model employs deep learning to detect irregular behavior in real time, enhancing data confidentiality in Big Data environments. In Software-Defined Networking (SDN), Liu et al. [9] developed DACAS, a dynamic ABAC model to secure northbound interfaces, addressing issues of permission control and resource sharing in SDN.

Blockchain-based access control has gained attention, particularly for IoT environments. Gong et al. [10] proposed SDACS, a blockchain-integrated model enabling decentralized, fine-grained access through smart contracts, reducing reliance on central servers and ensuring robust data sharing in IoT. Similarly, Alazab et al. [11] presented an LSTM-based Intrusion Detection System (IDS) for IoT that dynamically adjusts access permissions, detecting intrusions with high accuracy and a rapid response time. In cloud storage, Alharbe et al. [12] introduced a risk-based ABAC model tailored to dynamic data protection. By assessing subject, resource, and environment attributes, this model offers fine-grained security adjustments suitable for sensitive cloud data, such as medical records. Farhadighalati et al. [13] focused on human-centric access for Electronic Health Records (EHR), combining ABAC with risk assessments to secure healthcare data. Other notable advancements include MLCAC by Xiao et al. [14], a multi-layered model targeting insider threats through real-time monitoring and adaptive access decisions. For smart homes, Burakgazi et al. [15] extended ABAC by integrating biometric-based authentication, refining access control policies based on user verification scores. Zhong et al. [16] contributed to IoT edge security with SC-ABAC, a model using blockchain and smart contracts to manage access in decentralized environments. Lastly, Zhong et al. [17] enhanced RBAC with blockchain for dynamic, role-based access in data collaboration systems, achieving greater adaptability and security in organizational data access. These studies underscore the progression toward integrating ABAC with dynamic, context-aware technologies to strengthen security across IoT, cloud, and SDN platforms, demonstrating the effectiveness of hybrid models in complex digital environments.

III. Methodology

The methodology is structured to provide adaptive access permissions by analyzing user behavior and contextual data in real time. This approach enhances security by dynamically adjusting access permissions based on activity patterns, device information, and risk assessments derived from behavioral analytics. Fig. 1 illustrates the activity log workflow of the DACS, beginning with data collection and preprocessing, followed by feature extraction, model building, training, and risk assessment, ultimately leading to access control decisions and continuous monitoring.

First, Data Collection involves gathering user activity logs, which may include login times, device types, and other contextual data points. These logs, stored in SQL or NoSQL databases, are essential for understanding user behavior patterns and evaluating potential security risks. Next, Data Preprocessing is carried out to clean, convert, and standardize this raw data, ensuring its consistency and quality. In Python, for instance, preprocessing steps involve converting login times into a standardized datetime format using the pandas library, which simplifies temporal analysis. The following code snippet represents this step: defining a function that converts the 'login_time' column in user logs to a datetime format, ensuring consistency across entries.

This allows accurate analysis of time-based behavior patterns. Following preprocessing, Feature Extraction identifies key variables, such as login frequency, device type, and usage patterns. These extracted features provide a comprehensive profile of each user's typical behavior, which is essential for generating an accurate risk profile. Subsequently, a Behavioral Analytics Model is trained using machine learning frameworks like TensorFlow or PyTorch. This model, commonly a neural network, learns from historical user ac-

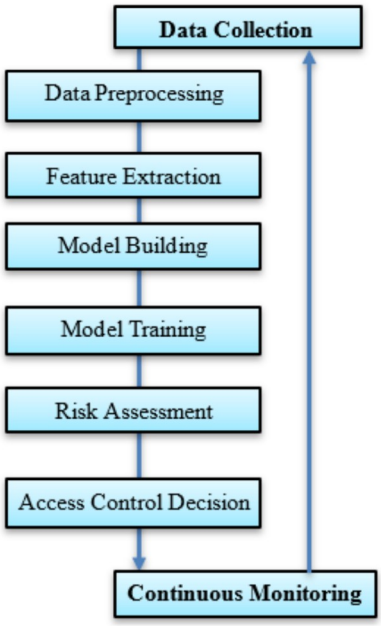

Fig 1. DACS Activity Log Workflow.

tivity data to compute a risk score for each access attempt. The risk score quantifies the likelihood that an access attempt is legitimate or anomalous. To enable real-time processing, Data Streaming is implemented using Apache Kafka, which streams user activity logs continuously to ensure the behavioral model is updated with the latest information. With this real-time data, DACS continuously evaluates and adjusts risk scores. When a user attempts to access a system, their behavior is compared to established patterns, and the Access Control Adjustment mechanism adapts permissions accordingly. For instance, if a high-risk score is detected (indicating unusual activity or potential threat), the system may restrict access or require additional verification. Conversely, low-risk scores allow seamless access, minimizing interruptions for legitimate users. The Visualization and Monitoring component completes the methodology, using tools like Matplotlib or Plotly to generate real-time graphs and reports. These visualizations provide system administrators with insights into user behavior trends and the effectiveness of the access control system. This comprehensive methodology ensures that DACS dynamically responds to potential threats, balancing security and usability in modern digital environments.

IV. System Implementation

The implementation of the system involves a layered approach that incorporates data collection, preprocessing, feature extraction, model development, and continuous monitoring to provide adaptive access permissions based on user behavior and contextual data. This architecture leverages machine learning techniques and real-time data processing to enhance security by dynamically adjusting access controls. Fig. 2 depicts the decision-making workflow in the DACS, starting from data collection and preprocessing through model building, training, and risk assessment. Based on real-time risk evaluation, the system adjusts access permissions dynamically, categorizing them as low, moderate, or high risk.

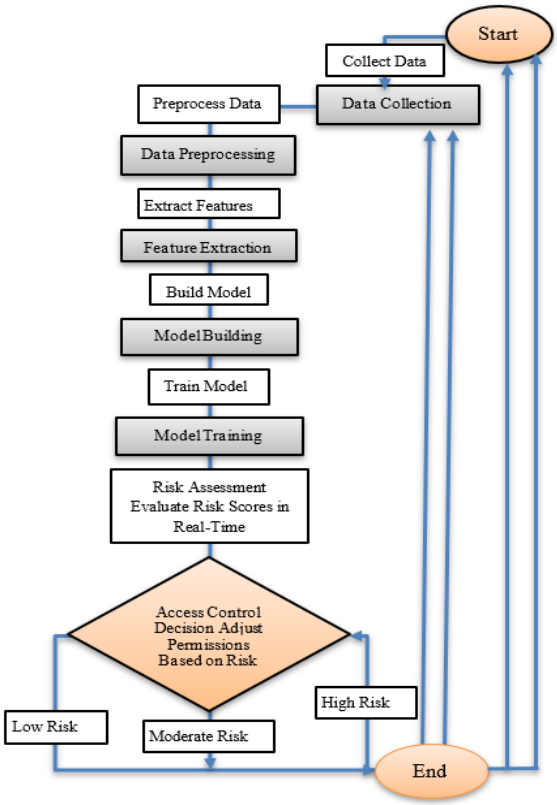

Fig 2. DACS Decision-Making Workflow.

Data collection forms the foundation, gathering user activity logs (e.g., login times, locations, devices) and contextual data (e.g., network conditions, time of access). This data, stored in SQL/NoSQL databases, enables behavioral pattern analysis and risk assessment. In Data Preprocessing, raw data is cleaned, normalized, and encoded, preparing it for model input. Feature Extraction then identifies key variables, such as time-based usage patterns and contextual risk factors, enhancing risk assessment capabilities. Model building involves developing a neural network using TensorFlow or PyTorch, with an input layer for features, hidden layers for complex pattern recognition, and an output layer that generates a risk score. The model is trained and optimized with metrics like accuracy and F1-score. Based on Risk Scoring, thresholds classify access attempts into low, moderate, or high-risk levels, with actions tailored accordingly. Access control adjustment dynamically modifies permissions in real time based on risk levels. Continuous monitoring updates user profiles and retrains the model as new data emerges. The system integrates software like Apache Kafka, SQL/NoSQL databases, and visualization tools, with cloud-based infrastructure and GPUs for scalability. In the Algorithm Workflow, data is streamed, preprocessed, and analyzed to produce risk-based access decisions, with actions

logged for auditing. Security is enforced through data encryption, secure authentication, and ISO/IEC 27001 compliance.

V. Results And Discussion

Fig. 3 illustrates the model's training and validation loss over 20 epochs, showing the model's learning progression. A decrease in training loss indicates the model's improved fit to the data, while fluctuations in validation loss reflect its generalization capacity on unseen data. Ideally, both losses should converge, with lower values signaling model effectiveness. However, substantial variance in validation loss suggests potential overfitting, necessitating adjustments.

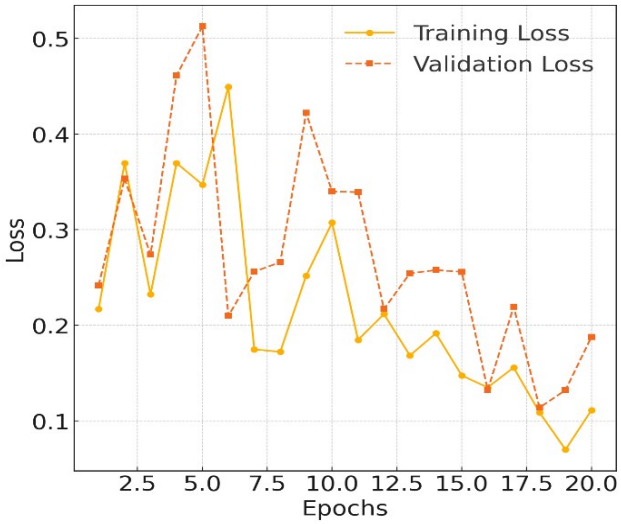

Fig 3. Training and Validation Loss over Epochs.

Fig. 4 shows the processing latency of system across 20 time intervals, indicating the response time for real-time data processing. Latency fluctuates between 100 ms and 300 ms, reflecting variations in system load and computational demand. Observing latency patterns helps identify any periods of high delay that could impact the system's responsiveness. These insights are essential for optimizing the model's efficiency and maintaining real-time adaptability.

Fig. 5 shows the Detection Accuracy comparison, with the static access control model at 70% and the DACS model at 87%. The reduced bar width highlights the difference in accuracy, demonstrating the improved detection capability of DACS. This comparison emphasizes DACS's advantage in accurately adapting to real-time behavioral changes, which enhances security by reducing the risk of unauthorized access.

Fig. 6 displays the throughput comparison between the static access control model and the DACS. Throughput, measured in requests per second, is significantly higher for the DACS model (220 requests/sec) compared to the static model (150 requests/sec). This improvement demonstrates DACS's efficiency in handling a larger volume of requests, essential for environments requiring rapid, real-time access control decisions.

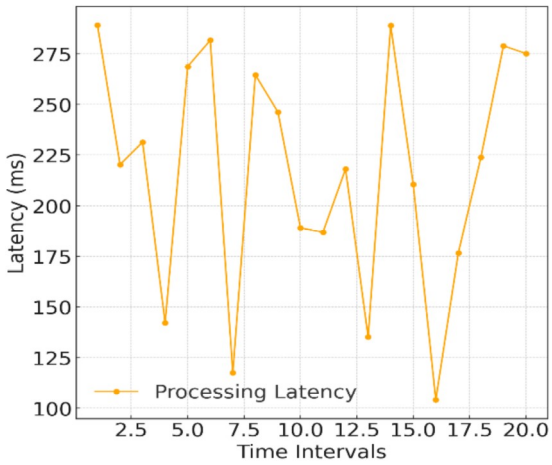

Fig 4. Real-Time Processing Latency over Time Intervals.

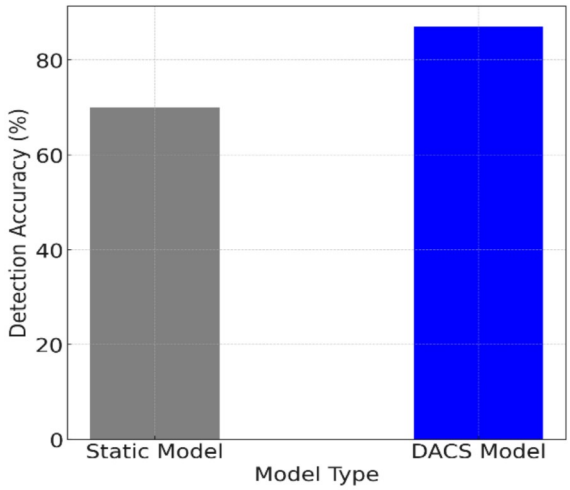

Fig 5. Detection Accuracy Comparison of Static and DACS Models.

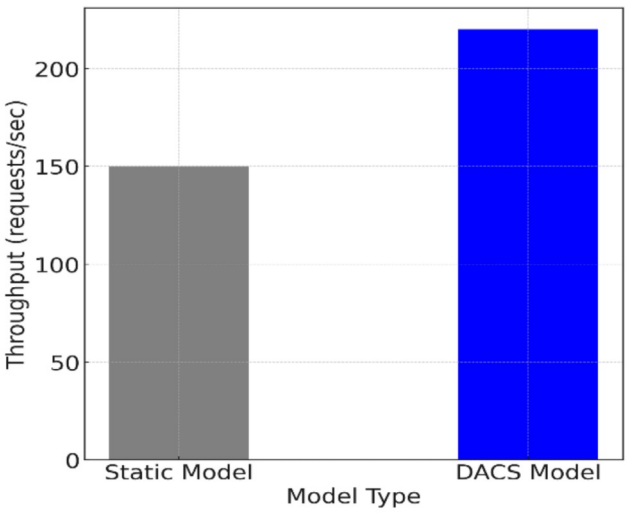

Fig 6. Throughput Comparison of Static and DACS Models.

VI. Conclusion

The DACS enhances cybersecurity by leveraging real-time behavioral analytics to adapt access permissions based on user activity, contextual data, and risk assessment. DACS gathers detailed user activity logs, applies preprocessing techniques like normalization and encoding, and extracts crucial features related to time, behavior patterns, and contextual risk factors. These features are processed through a neural network model built on frameworks such as TensorFlow or PyTorch to compute dynamic risk scores for each access attempt. Based on these scores, DACS adjusts permissions: low-risk scores allow seamless access, moderate-risk scores prompt additional authentication, and high-risk scores restrict access. Continuous data streaming via Apache Kafka ensures that real-time behavioral changes are promptly reflected in access decisions, allowing for adaptive, risk-based responses. This system showcases scalability and responsiveness, offering a practical, intelligent solution to evolving cybersecurity threats. DACS demonstrates the efficacy of integrating machine learning with access control, providing a robust and flexible security framework for modern, high-demand environments.

References

[1] Ameer, Safwa, James Benson, and Ravi Sandhu. "An attribute-based approach toward a secured smart-home IoT access control and a comparison with a role-based approach." *Information* 13, no. 2 (2022): 60.

[2] Ameer, Safwa, James Benson, and Ravi Sandhu. "Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT." *IEEE Transactions on Dependable and Secure Computing* 20, no. 5 (2022): 4032-4051.

[3] Burakgazi Bilgen, Melike, Osman Abul, and Kemal Bicakci. "Authentication-enabled attribute-based access control for smart homes." *International Journal of Information Security* 22, no. 2 (2023): 479-495.

[4] Ameer, Safwa. "User-To-Device Access Control Models for Cloud-Enabled IoT with Smart Home Case Study." PhD diss., The University of Texas at San Antonio, 2021.

[5] Ameer, Safwa, James Benson, and Ravi Sandhu. "The EGRBAC model for smart home IoT." In *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*, pp. 457-462. IEEE, 2020.

[6] Huang, Haoxiang, Jianbiao Zhang, Jun Hu, Yingfang Fu, and Chenggang Qin. "Research on distributed dynamic trusted access control based on security subsystem." *IEEE Transactions on Information Forensics and Security* 17 (2022): 3306-3320.

[7] Kim, Hwimin, Dae-Kyoo Kim, and Alaa Alaerjan. "ABAC-based security model for DDS." *IEEE Transactions on Dependable and Secure Computing* 19, no. 5 (2021): 3113-3124.

[8] Vijayanand, S., and S. Saravanan. "A deep learning model based anomalous behavior detection for supporting verifiable access control scheme in cloud servers." *Journal of Intelligent & Fuzzy Systems* 42, no. 6 (2022): 6171-6181.

[9] Liu, Yifan, Bo Zhao, Yang An, and Jiabao Guo. "DACAS: integration of attribute-based access control for northbound interface security in SDN." *World Wide Web* 26, no. 4 (2023): 2143-2173.

[10] Gong, Qinghua, Jinnan Zhang, Zheng Wei, Xinmin Wang, Xia Zhang, Xin Yan, Yang Liu, and Liming Dong. "SDACS: Blockchain-Based Secure and Dynamic Access Control Scheme for Internet of Things." *Sensors* 24, no. 7 (2024): 2267.

[11] Alazab, Moutaz, Albara Awajan, Hadeel Alazzam, Mohammad Wedyan, Bandar Alshawi, and Ryan Alturki. "A novel IDS with a dynamic access control algorithm to detect and defend intrusion at IoT nodes." *Sensors* 24, no. 7 (2024): 2188.

[12] Alharbe, Nawaf, Abeer Aljohani, Mohamed Ali Rakrouki, and Mashael Khayyat. "An access control model based on system security risk for dynamic sensitive data storage in the cloud." *Applied Sciences* 13, no. 5 (2023): 3187.

[13] Farhadighalati, Nastaran, Jose Barata, Sanaz Nikghadam-Hojjati, and Eda Marchetti. "Behavioral and Human-Centric Access Control Model in XACML Reference Architecture: Design and Implementation of EHR Case Study." In *Technological Innovation for Human-Centric Systems: 15th IFIP WG 5.5/SOCOLNET Advanced Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2024, Caparica, Portugal, July 3-5, 2024, Proceedings*, vol. 716, p. 192. Springer Nature, 2024.

[14] Xiao, Lifang, Aimin Yu, Hanyu Wang, Lixin Zhao, and Dan Meng. "MLCAC: Dynamic Authorization and Intelligent Decision-making towards Insider Threats." In *2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 407-412. IEEE, 2024.

[15] Burakgazi Bilgen, Melike, Osman Abul, and Kemal Bicakci. "Authentication-enabled attribute-based access control for smart homes." *International Journal of Information Security* 22, no. 2 (2023): 479-495.

[16] Zhonghua, Chen, S. B. Goyal, and Anand Singh Rajawat. "Smart contracts attribute-based access control model for security & privacy of IoT system using blockchain and edge computing." *The Journal of Supercomputing* 80, no. 2 (2024): 1396-1425.

[17] Zhong, Tao, Junsheng Chang, Peichang Shi, Linhui Li, and Fei Gao. "Dyacon: Jointcloud dynamic access control model of data security based on verifiable credentials." In *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, pp. 336-343. IEEE, 2021.