# Fighting Insurance Fraud with Hybrid AI/ML Models: Discuss the potential for combining approaches for improved insurance fraud detection

Venkata Ramana Saddi,
Technology Lead,
ACE American Insurance - Chubb Group,
Raleigh, NC, USA
ramana.saddi@outlook.com

Bhagawan Gnanapa,
AI/ML Architect,
SmartTrak AI,
Holly Springs, NC, USA
bhagawan.reddy@gmail.com

Swetha Boddu,
Senior Consultant, Perficient Inc.,
Raleigh, NC, USA
boddu.swetha@gmail.com

J.Logeshwaran,
Department of ECE, Sri Eshwar College of Engineering,
Coimbatore, Tamil Nadu, INDIA
eshwaranece91@gmail.com

2023 4th International Conference on Communication, Computing and Industry 6.0 (C216) | 979-8-3503-2732-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/C2I659362.2023.10431155

***Abstract*— The emergence of hybrid AI/ML fashions has allowed for advanced fraud detection within the insurance enterprise. Combining a couple of AI/ML methods including supervised and unsupervised studying, deep studying, and herbal language processing, can offer a effective set of tools to hit upon fraudulent claims. Supervised getting to know can discover patterns in claims facts that might indiciate fraud, while unsupervised gaining knowledge of can alert to surprising changes in behavior or outliers in behavior. Deep mastering can analyze enormous quantities of information to discover suspicious claims styles, and herbal language processing can speedy seek massive information units for suspicious keywords. Hybrid AI/ML fashions can help perceive even the most state-of-the-art fraud operations and stumble on anomalies before they grow to be too massive to manipulate. these fashions also can be leveraged to hit upon fraud developments before they become too full-size, making an allowance for early prevention methods. by way of leveraging disparate AI/ML strategies, insurers are higher able to shield themselves from fraudulent conduct and maximize the efficiency of their fraud detection tactics..**

***Keywords*— massive, detection, information, maximize, knowledge**

## I. Introduction

The potential for combining particular AI/ML fashions with up-to-date insurance fraud detection is massive, specifically as more recent AI/ML models have become increasingly sophisticated[1]. Many present-day AI/ML procedures for up-to-date fraud detection rely on supervised learning of up-to-date known fraud styles; combining a couple of AI/ML fashions can help improve detection accuracy. For example, hybrid techniques that integrate supervised studying with unsupervised up to date can offer better accuracy prices[2-6]. Unsupervised mastering styles can assist in discovering more excellent diffused patterns inside the records, allowing for better detection of lesser-regarded types of fraud. Similarly, combining one-of-a-kind AI/ML models permits stepped-forward generalization, as the models are more likely to date and discover new fraud styles as they emerge[7-9]. With no longer supervised learning fashions but also unsupervised up-to-date fashions, neural networks, and more, insurers can better identify new patterns of fraudulent activity.

Moreover, combining AI/ML models with vital records units and advanced analytics can offer a more complete and up-to-date update of fraudulent interest[10]. Insurers are up-to-date. Additionally, don't forget to update the use of actual-time information streams for up-to-date fraud detection. By using streaming facts in up-to-date time, insurers can gather records and quickly hit upon probable fraudulent activity earlier than it could cause up-to-date harm[11-14]. Combining more than one AI/ML approach for progressed insurance fraud detection holds splendid ability. AI/ML fashions can be used to uncover complicated styles in statistics that traditional models may additionally overlook[15]. With deep studying techniques, including updated convolutional neural networks (CNNs) and recurrent neural networks (RNNs), insurance groups can discover extra subtle fraud styles through supervised learning that models might not have been updated find[16].

Furthermore, AI/ML may identify potentially fraudulent cases faster and more accurately than conventional strategies. For example, anomaly detection algorithms may be used to update unmarried anomalous hobby styles with better accuracy than the guide or rule-up-to-date tally updated methods utilized by coverage corporations[17-18]. Machine up-to-date strategies, which include supervised and unsupervised clustering, could also become aware of abnormally excessive claims for a particular demographic or region, helping insurers flag doubtlessly fraudulent claims faster. Combining a couple of AI/ML fashions can also carry extra accuracy in updated insurance fraud detection efforts. AI/ML models could be used in up-to-date significant quantities of records to become aware of anomalies. The construction diagram has shown in the following fig.1

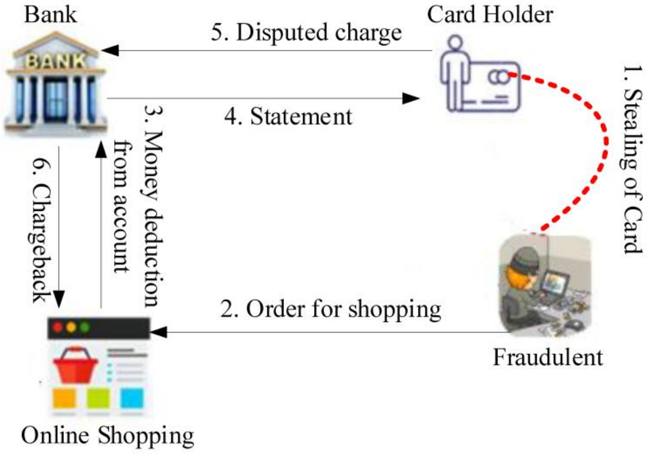

Fig. 1. Construction diagram

979-8-3503-2732-8/23/$31.00 ©2023 IEEE

In contrast, traditional fashions, logistic regression, and decision timber might be used to discover danger to up-to-date fraudulent claims[19]. By combining the two, insurers have up-to-date advantages and more specified insights into how every model deciphers statistics.

1. The ability to combine multiple AI/ML processes for stepped-forward coverage fraud detection is gigantic. By blending statistics from several resources, AI-pushed detection models can quickly and accurately become aware of suspicious styles. With proper optimization, they may be best tuned up-to-date, converting fraud tendencies.

2. At the core of such hybrid AI/ML models is an intelligent structure combining rule-primarily based systems, supervised up-to-date and unsupervised gaining knowledge of models. Rule-based systems offer coverage for very precise eventualities; at the same time, managed up-to-date techniques are desirable at spotting patterns but tend to bias up-to-date education statistics. Unsupervised learning techniques can hit upon dense areas in the records, which is particularly useful when faced with sudden events not found in hooked-up models. Every kind can be tuned to updated exceptional scenarios, leading to up-to-date enhanced insurance for various fraud types.

3. Moreover, using natural language processing (NLP) strategies can, in addition, boost the coverage of a detection model and allow insurers to apprehend nuances that may be blind spots for simple rule-up-to-date models. It may be used to discover each specific and implicit fraudulent sport by correlating deceitful language or suspicious phraseology present in submitted documents and using sentiment analysis techniques updated hit upon purple-flag expressions.,

## II. Related Works

Btoush, E. A. L. M., et al. [1] A systematic overview of the literature on credit score card cyber fraud detection using systems and deep studying is an evaluation of scientific research, articles, and different information that examines how synthetic intelligence (AI) and deep mastering strategies are being used to stumble on and save you cyber fraud related to credit score playing cards. It's by far a complete and particular observation of the exclusive varieties of fraud detection techniques that have been studied, how powerful they are, the gaps in cutting-edge generation, and what still wishes to be explored and advanced. The evaluation will cover various techniques, including predictive analytics, anomaly detection, clustering, statistics retrieval, and different AI and deep knowledge of techniques. It will also look at how these techniques are deployed in exceptional contexts and to distinct fulfillment ranges.

Jabeur, S. B., et al. [2]Synthetic intelligence (AI) has been used to detect faux critiques in various ways, and this approach to bogus review detection has visibly developed interest in recent years. One AI-primarily based approach used in fake assessment detection is bibliometric analysis. This technique includes assessing the content of reviews and analyzing them to figure out patterns or features associated with bogus evaluations. Through natural language processing and gadget-getting-to-know strategies, bibliometric analysis can be used to detect evaluations that lack positive traits frequently found in authentic critiques, including non-public language or emotion.

Dwivedi, Y. K., et al. [3]ChatGPT is the latest improvement in the AI era specifically designed to generate natural, human-like conversations with computer programs. With ChatGPT, researchers can now create popular communication scripts and automatically respond to each user entry, considering more dynamic, practical conversations between computer systems and humans than previously viable. This era has opened up limitless possibilities for research and valuable packages, ranging from automatic customer support and medical sessions to non-public assistants and online schooling. It also holds capability implications for psychology, sociology, discourse evaluation, and linguistics. With this new era, it's miles feasible to examine the structure and exceptional of conversations between people and machines, as well as their impact on present social dynamics and relationships. Standard, ChatGPT affords both thrilling opportunities and demanding situations for researchers. It'll be exciting to see how this generation will continue to shape our know-how of language and communiqué.

Cox Jr, L. A. et al. [4]AI-ML for selection and hazard evaluation uses AI and gadget learning (ML) to help with the selection-making and danger evaluation technique. AI and ML are increasingly being deployed to enable quicker and greater correct risk-primarily based evaluation while incorporating elements of normative decision-making, including uncertainty and desire control. This combination of techniques can significantly enhance our risk information from a qualitative and quantitative perspective. The aim of AI-ML for choice and threat analysis is to increase the accuracy and velocity of decisions and reduce chance while increasing decision-makers self-belief. Through AI and ML, organizations can make choices quicker, more accurately, and with extra self-belief. This era also can help businesses reap higher results while assessing risks and making choices in uncertain, complicated environments.

Capuano, N., et al. [5] have discussed the concepts and Design Thinking Innovation addressing global financial wishes is a look at Innovation in financing and its potential role in the global financial system. The research examines the modern nation of the worldwide economic quarter, the demanding situations it faces, and investigates economic Innovation's possibilities. The report affords a top-level view of the concept, how it's miles applied, and why it's vital. It also outlines the ability to create modern answers to assist in fostering financial inclusion and increase the sector's maximum disadvantaged individuals, households, and communities. It also highlights the importance of collaboration and integration between stakeholders to ensure a hit outcome. The file is meant to encourage, in addition, investigation and exploration into the capability of layout thinking and Innovation in the international financial zone.

## III. Proposed Model

Combining more than one AI/ML procedure for progressed coverage fraud detection has the capability for advanced detection accuracy and actual-time detection. Potential approaches encompass integrating unsupervised knowledge of algorithms such as clustering and anomaly detection with supervised mastering algorithms, including selection trees and random forests. Clustering can uncover previously unknown similarities and patterns among statistics. Anomaly detection is beneficial for detecting strange behavior.

$$i_j = \{i_1, i_2, i_3......, i_n\} \quad (1)$$

$$j_o = \{j_1, j_2, j_3......, j_m\} \quad (2)$$

Supervised studying algorithms can be trained to understand fraud-related practices and properly require categorized datasets to stumble on scams. Combining one-of-a-kind algorithms that hit upon ruse in exclusive methods can provide security professionals with more excellent, comprehensive, and accurate outcomes than they may get from an unmarried set of rules. For example, combining unsupervised gaining knowledge of and supervised mastering algorithms can offer insights into fraudulent activities that wouldn't be detected using either set of governments alone.

$$M = i_j + j_i \quad (3)$$

Moreover, leveraging hybrid AI/ML procedures may allow computerized fraud detection in actual time, a functionality that is important for identifying and preventing capacity fraud earlier than it takes region. The algorithm has shown in the following:

```
Insurance fraud detection Algorithm
Step.1    (A, B, C, B) – Some parameter
Step.2    N – Another parameter
Step.3    K – Yet another parameter
Step.4    N – Yet another parameter
Step.5    Do
Step.6    For j=1:n
Step.7    Loop definition.
Step.8    While(condition<N)
Step.9    For j=1:n
Step.10   Loop definition
Step.11   Some more text
Step.12   Some more text
Step.13   For j=1:n
Step.14   For s=1:k
Step.15   Loop definition
Step.16   Return (some variable)
```

## A. Surveys on Explainable Artificial Intelligence

By combining more than one AI/ML method, insurance corporations can create more accurate and advanced fraud detection models for catching fraudulent activity. The combination of AI/ML models allows a variety of rule-based and unsupervised models (e.g., anomaly detection) that may be utilized in live performance to identify subtle patterns in purchaser behavior that might suggest fraud.

$$j(i) = j_1(i) * j_2(i) \quad (4)$$

$$i(j) = i_1(j) * i_2(j) \quad (5)$$

With admission to more excellent data units (e.g., recorded voice calls, facial recognition, etc.), superior algorithms can research more sophisticated styles, which may be used to perceive anomalies, discover complex fraud schemes, and detect threats from newly rising fraud jewelry. The functional block diagram has shown in the following fig.2

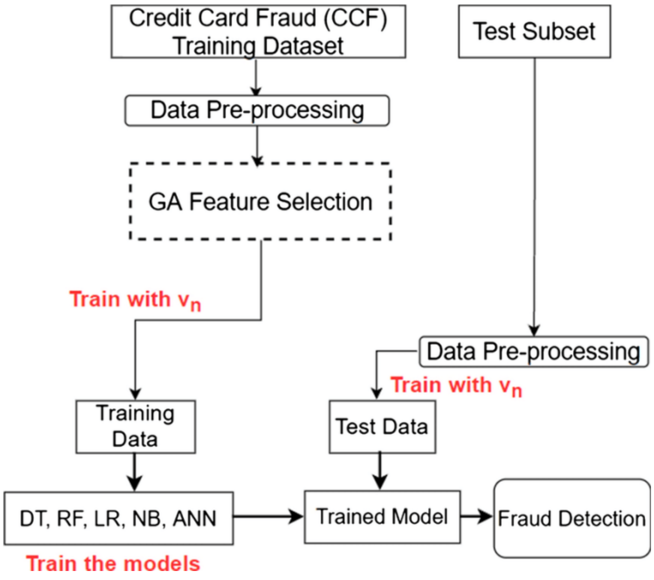

Fig. 2. Functional block diagram

Additionally, some ML models allow insurance organizations to lessen the capability for fake positives, which could store money and time within an extended period. Over time, combining more than one AI/ML fashion promises higher accuracy, quicker processing speeds, and better insurance against rising sorts/developments of fraud that might not be without problems detected from conventional techniques.

## B. Surveys on Artificial Intelligence Applications in Cybersecurity

By combining more than one AI/ML process in coverage fraud detection, the capacity to detect styles in fraud becomes more accurate because of the increase in the depth and breadth of statistics being tested. For instance, combining supervised and unsupervised learning and herbal language processing blended with laptop imagination and prescient may also bring about extraordinarily correct fraud detection. The concept is to apply an expansion of fashions and methods, constantly imparting comments, to construct a higher version that may more accurately come across fraud instances.

$$j(i) = \{i_1 * j_1(i) + i_2 * j_2(i) + ..... + j_i * i_j(j)\} \quad (6)$$

$$M_j = \sum_{j=1}^{\infty} i_{x(j-1)} + j_{j(i-1)} \quad (7)$$

The operational flow diagram has shown in the following fig.3

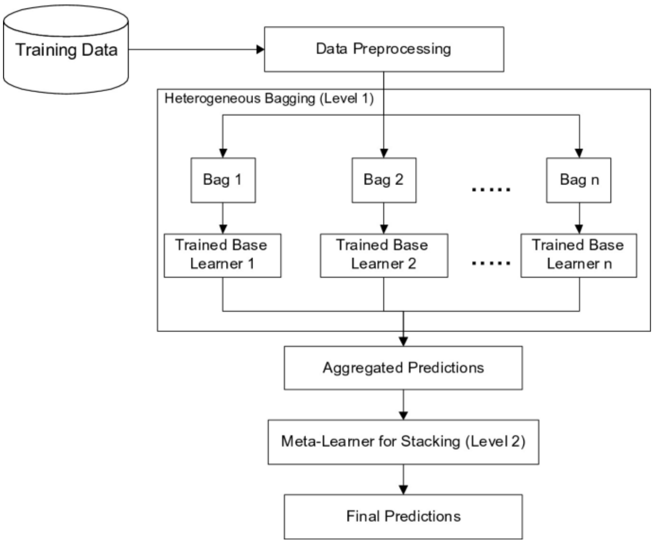

Fig. 3. Operational flow diagram

Additionally, hybrid AI/ML fashions may be designed using transfer mastering, in which information gained from solving one problem may be used to resolve any other. The transfer learning technique can accelerate the getting-to-know approach and make the version more robust.

### C. *XAI Surveys in Cybersecurity*

Combining more than one AI/ML strategy can yield more accurate and reliable insurance fraud detection predictions. These approaches can also consist of using computer vision to analyze the pics of submitted guidelines and payments, gaining knowledge to become aware of styles and locate anomalies, and using herbal language processing (NLP) to research text and stumble on suspicious phrases or principles.

$$M = \left\{ \frac{j(i)+i(j)}{i(j,i)} \right\} \tag{8}$$

$$M = \left\{ \frac{(j_1(i)*j_2(i))+(i_1(j)*i_2(j))}{j(j,i)*i(j,i)} \right\} \tag{9}$$

The hybrid version has to be designed to leverage the strengths of every individual approach to beautify the general accuracy of fraud detection.

$$M = \{i_1, i_2, i_3......, i_n\} + \{j_1, j_2, j_3......, j_m\} \tag{10}$$

Additionally, AI/ML can be used to system and analyze big datasets faster and more efficiently, enabling insurers to discover and deal with fraudulent activities more quickly and effectively.

## IV. Results and Discussion

An ML version can then examine the data in addition to helping affirm the suspected fraud and offer more excellent information about it. By combining distinct AI and ML techniques, coverage businesses can benefit from more profound insights into their claims, permitting them to detect and prevent fraud.

### A. *Intrusion Detection Systems*

Hybrid AI/ML models use strategies from each synthetic Intelligence (AI) and gadget getting to know (ML). AI models use rule-based structures to locate and analyze styles in statistics, offering insights and knowledge that may be used to identify fraud. Fig.4 shows the Intrusion Detection Systems

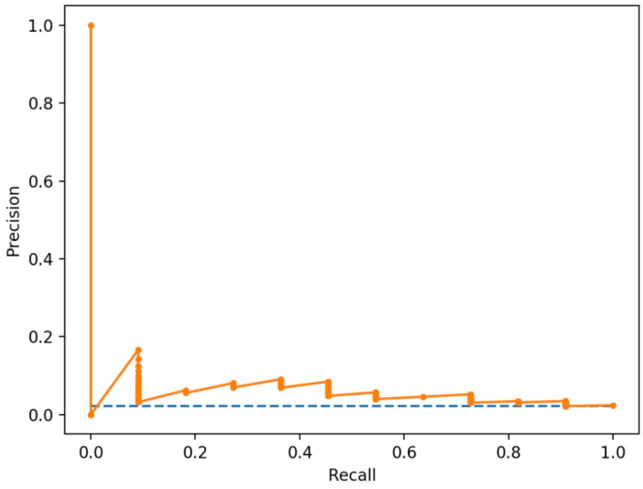

Fig. 4. Intrusion Detection Systems

ML models use supervised and unsupervised algorithms to analyze information and pick out trends that may suggest the presence of fraud. Combining both strategies can improve coverage fraud detection, as AI models can identify capacity fraud, and ML fashions can verify those instances and provide more excellent targeted analysis. For example, an AI version can identify anomalies inside the records, including discrepancies between stated and actual expenses, which can suggest capability fraud.

### B. *Malware Detection*

Combining a couple of tactics of AI/ML can significantly improve coverage fraud detection, considering that every method brings its strengths and particular insights. For instance, the usage of supervised device studying algorithms inclusive of selection trees or random forests can look into unique features of a declaration that might factor into feasible fraud, along with the amount of the claim cost, the claimant's beyond payment records, or even the location or geographic vicinity the claimant claims from. Fig.5 shows the Malware Detection.

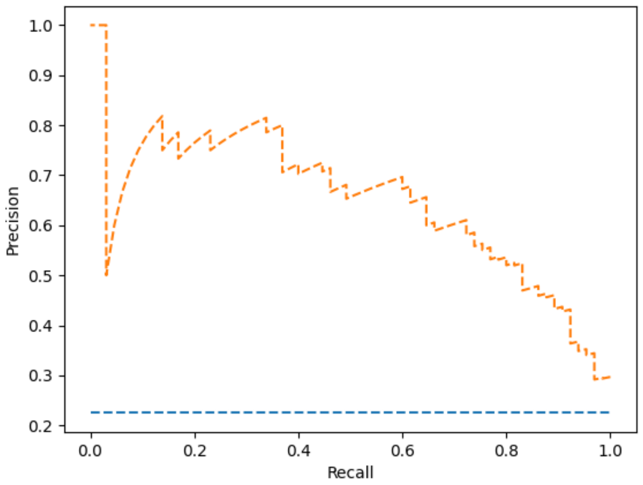

Fig. 5. Malware Detection

Then again, unsupervised strategies consisting of clustering or anomaly detection may be used to pick out suspicious businesses of claims or detect outlier or unusual claims. Combining those methods can allow for an extra complete analysis, identifying both styles of fraud as well as diffused variations within a particular fraud class. Additionally, combining multiple tactics, particularly when tuned with tuning and better training statistics, can impact fraud detection's overall performance. Fig.6 shows the Phishing and Spam Detection

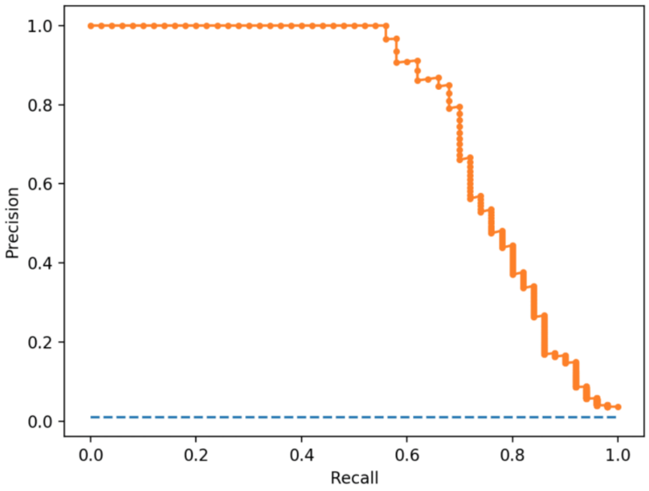

Fig. 6. Phishing and Spam Detection

### C. *Phishing and Spam Detection*

Using more than one AI/ML algorithm in a hybrid method can provide stepped-forward overall performance in detecting coverage fraud. A mixture of supervised and unsupervised models, which include neural networks, help vector machines, choice trees, and clustering algorithms, may be used collectively to perceive outlier and suspicious conduct. For instance, supervised models may be used to classify categorized statistics, and unsupervised fashions can identify outliers or suspicious patterns in transactional statistics. Moreover, AI/ML may be used to efficiently stumble on fraudulent styles in customer claims by reviewing textual content messages and documents. By combining more than one AI/ML fashion, agencies can come across outliers in records much faster, significantly reduce the number of fake positives, and correctly classify fraud.

### D. *BotNet Detection*

The capability for combining multiple AI/ML strategies for advanced coverage fraud detection is pretty excessive. Fig.7 shows the BotNet Detection.

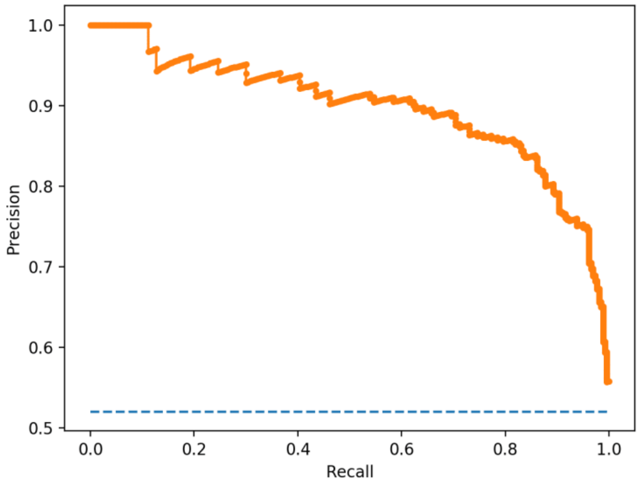

Fig. 7. BotNet Detection

Combining AI/ML models can help locate severe instances of fraud wherein a number of the styles used by conventional models may not be capable of capturing. If AI/ML fashions are utilized collectively in parallel, they could evaluate patterns and assist in picking out more diffused and sophisticated tries of fraudulent behavior.

## V. Conclusion

The examination of fighting coverage Fraud with Hybrid AI/ML models shows that combining more than one AI/ML strategy can notably enhance the accuracy of fraud detection given the complexity and volume of records to the system in preventing fraud within the current virtual global. Specifically, leveraging advanced gadgets to gain knowledge of algorithms in specific combinations can decrease fake positives, lessen the manual attempts of fraud inspectors, and maximize the accuracy of detecting fraudulent claims. Additionally, hybrid AI/ML fashions can provide personalization of fraud detection structures to stumble on more complicated fraud patterns in actual time. By leveraging multiple AI/ML models together in place of a single model, insurance fraud detection systems can't simply be extra correct; they can also be more powerful. As such, hybrid AI/ML fashions are seen as a potentially helpful device in fighting fraud and decreasing company losses..

## References

[1] Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.

[2] Jabeur, S. B., Ballouk, H., Arfi, W. B., & Sahut, J. M. (2023). Artificial intelligence applications in fake review detection: Bibliometric analysis and future avenues for research. Journal of Business Research, 158, 113631.

[3] Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., ... & Wright, R. (2023). “So what if ChatGPT wrote it?” Multidisciplinary perspectives on opportunities, challenges and

implications of generative conversational AI for research, practice and policy. International Journal of Information Management, 71, 102642.

[4] Cox Jr, L. A. (2023). AI-ML for Decision and Risk Analysis: Challenges and Opportunities for Normative Decision Theory.

[5] Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cybersecurity: A survey. IEEE Access, 10, 93575-93600.

[6] Martínez, B., Allmendinger, R., Khorshidi, H. A., Papamarkou, T., Feitas, A., Trippas, J., ... & Benson, K. (2023). Mapping the State of the Art: Artificial Intelligence for Decision Making in Financial Crime. Cybersecurity for Decision Makers, 199-213.

[7] Heidari, A., Navimipour, N. J., & Unal, M. (2022). Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: A systematic literature review. Sustainable Cities and Society, 104089.

[8] Eluwole, O. T., & Akande, S. (2022, July). Artificial Intelligence in Finance: Possibilities and Threats. In 2022 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT) (pp. 268-273). IEEE.

[9] Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Computer Science, 9, e1278.

[10] Heidari, A., Jafari Navimipour, N., Unal, M., & Toumaj, S. (2022). Machine learning applications for COVID-19 outbreak management. Neural Computing and Applications, 34(18), 15313-15348.

[11] Javed, A. R., Ahmed, W., Pandya, S., Maddikunta, P. K. R., Alazab, M., & Gadekallu, T. R. (2023). A survey of explainable artificial intelligence for smart cities. Electronics, 12(4), 1020.

[12] Molnár, B., Pisoni, G., Kherbouche, M., & Zghal, Y. (2023). Blockchain-Based Business Process Management (BPM) for Finance: The Case of Credit and Claim Requests. Smart Cities, 6(3), 1254-1278.

[13] Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2023). Artificial intelligence for the metaverse: A survey. Engineering Applications of Artificial Intelligence, 117, 105581.

[14] Chakraborty, A., Biswas, A., & Khan, A. K. (2022). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. arXiv preprint arXiv:2209.13454.

[15] Azzutti, A. (2022). AI trading and the limits of EU law enforcement in deterring market manipulation. Computer Law & Security Review, 45, 105690.

[16] Huynh-The, T., Pham, Q. V., Pham, X. Q., Nguyen, T. T., Han, Z., & Kim, D. S. (2022). Artificial intelligence for the metaverse: A survey. arXiv preprint arXiv:2202.10336.

[17] Shaheen, M., Farooq, M. S., Umer, T., & Kim, B. S. (2022). Applications of federated learning; Taxonomy, challenges, and research trends. Electronics, 11(4), 670.

[18] Gupta, K., Jiwani, N., Sharif, M. H. U., Datta, R., & Afreen, N. (2022, November). A Neural Network Approach For Malware Classification. In 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) (pp. 681-684). IEEE.

[19] Jiwani, N., & Gupta, K. (2018). Exploring Business intelligence capabilities for supply chain: a systematic review. Transactions on Latest Trends in IoT, 1(1), 1-10.