Research Journal of Computer Systems and Engineering (RJCSE)
Volume 4 Issue 1 (2023) | Pages: 102 – 109 | e-ISSN: 2230-8571; p-ISSN: 2230-8563
https://doi.org/10.52710/rjcse.68

Predictive Analytics for Cyber Threats to Enhance Security in the Cyber Supply Chain

Received: 30 March 2023; Revised: 18 May 2023; Accepted: 16 June 2023

Mrs. Pranali S. Kshirsagar
Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune - India
pranali.kshirsagar@viit.ac.in

Dr. Avinash M. Pawar
Ph.D. Mechanical Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune
avinash.m.pawar@bharatividyapeeth.edu

Abstract

Using predictive analytics is a key part of making the computer supply chain safer because it helps companies find and stop threats before they happen. Predictive analytics uses complex algorithms and machine learning to look through huge amounts of data for trends and outliers that could point to cyber dangers. Businesses can stay ahead of cyber attackers and keep their digital assets safe with this method. In the online supply chain, one of the best things about prediction analytics is that it can find new threats before they become full-blown attacks. Predictive analytics looks at past data, current trends, and other factors to be able to guess possible computer dangers and weak spots. In turn, this lets businesses take strategic steps to lower these risks, like fixing security holes or adding more protections. Predictive analytics can also improve the cyber supply chain's ability to respond to incidents. Predictive analytics looks at data from many places, like network logs, endpoint devices, and security monitors, to help find and rank possible security events. This lets companies react quickly and effectively to cyberattacks to lessen their effects. The prediction analytics is a great way to make the online supply chain safer. Using advanced algorithms and machine learning, businesses can find and stop cyber dangers before they happen, keep their digital assets safe, and boost their total security.

Keywords

Predictive analytics, Cyber supply chain, Cybersecurity, Machine learning, Threat detection

1. Introduction

The online supply chain is a complicated web of systems and processes that work together to make it possible for things, services, and information to move around the internet. As businesses depend more and more on digital tools to run, the online supply chain has become an important part of their processes. But because of this, businesses are open to many types of cyber risks, such as data leaks, ransomware attacks, and supply chain compromises [1]. To deal with these issues, businesses are using predictive analytics, a strong tool that uses advanced algorithms and machine learning to look at huge amounts of data and find trends that could point to cyber risks. By using prediction analytics in the cyber supply chain, businesses can find and reduce risks before they happen, keep their digital assets safe, and improve their overall security [2].

One of the best things about prediction analytics in the cyber supply chain is that it can find new threats before they become full-on attacks [3]. Predictive analytics looks at past data, current trends, and other factors to guess what computer dangers and weaknesses might happen. This means that companies can proactively lower these risks by doing things like fixing security holes or adding more security measures. Additionally, prediction analytics can also improve the cyber supply chain's ability to respond to incidents. Predictive analytics can help find and rank possible security events by looking at data from many sources, such as network logs, endpoint devices, and security monitors. This lets businesses react quickly and effectively to cyberattacks and lessen their effects [4].

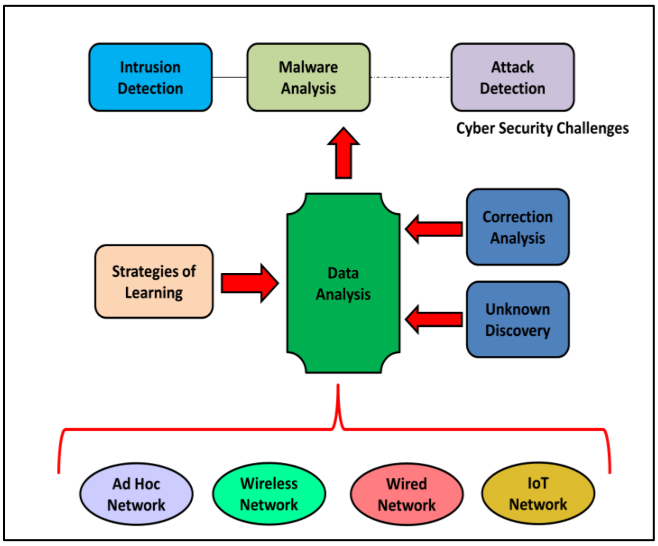

Figure 1: Overview of Predictive Analytic for cyber supply chain

Predictive analytics can help businesses improve their general security in addition to making it easier to find threats and deal with incidents. Predictive analytics looks at data from all parts of the cyber supply chain to find weak spots and suggest ways to make things better [5]. This could mean putting in place stricter rules for entry, doing regular security checks, or improving training programs for employees. In general, prediction analytics is a great way to make the online supply chain safer. Organizations can effectively find and stop cyber dangers, protect their digital assets, and improve their overall security by using advanced algorithms and machine learning techniques. Predictive analytics will become more and more important in protecting the cyber supply chain and businesses from cyber dangers as they continue to rely on digital technologies to run their businesses [6].

2. Related Work

The area of cyber danger predictive analytics is changing quickly. More and more study and related work is being done to make the cyber supply chain safer. Predictive analytics is getting better in this area thanks to progress in a number of important areas of study and development [7]. One area of work that is relevant is making powerful machine learning systems that can find threats. Researchers are looking into new ways to look at data from the cyber supply chain in order to find trends and outliers that could point to possible threats. For instance, academics have created machine learning models that can look at data about network activity to find strange trends that could be signs of an attack. These models can help businesses find and deal with threats in their supply chains before they happen.

Predictive analytics [8] being added to current security systems and tools is another area of work that is connected. Scientists are looking into ways to add predictive analytics to security tools like intrusion detection systems (IDS), security information and event management (SIEM) systems, and more. Organizations can better find and deal with cyber dangers in real time by using predictive analytics. This makes the cyber supply chain safer overall. Researchers are also looking into how prediction analytics can be used to handle and analyze risk in the cyber supply chain. Predictive analytics [9] can help businesses find and highlight areas of risk by looking at data from all parts of the supply chain, such as partner connections, data flows, and access rules. This can help companies better decide how to use their resources to lower these risks and make the online supply chain safer. Coming up with predictive analytics models for cyber threat information is another area of work that is connected. Scientists are looking into how to use predictive analytics to look at a lot of threat intelligence data and find useful information. Companies can better understand new dangers and trends by using predictive analytics to look at threat intelligence data. This lets them protect their supply chain before problems happen.

Also, experts are looking into how prediction analytics can be used to help with responding to incidents in the computer supply chain [10]. Organizations can make models that can help them figure out how likely and bad future security incidents will be by looking at data from past incidents and using predictive analytics methods. This can help businesses get ready for and deal with cyber dangers better, which lowers the risk to the cyber supply chain as a whole. Overall, the field of predictive analytics for cyber risks is moving forward quickly, with experts looking into new ways to make the cyber supply chain safer [11]. Researchers are helping to protect organizations from cyber threats and improve security in the cyber supply chain by creating new advanced machine learning algorithms and integrating predictive analytics into existing security frameworks. They are also using predictive analytics for risk assessment and incident response.

Table I: Related Work Sumamry

Method	Finding	Approach	Limitation	Advantages
Machine Learning Algorithms	Detecting anomalies in network traffic	Analyzing network traffic data	Requires labeled data for training	Can proactively identify and mitigate threats
Integration with SIEM	Real-time threat detection	Integrating predictive analytics into SIEM	May require significant resources to implement	Improves real-time threat detection
Risk Assessment	Identifying and prioritizing risks	Analyzing data from across the supply chain	Limited by the quality and availability of data	Enables effective resource allocation
Threat Intelligence Analysis	Extracting actionable insights	Analyzing large volumes of threat intelligence	Requires advanced analytics skills	Helps understand emerging threats and trends
Incident Response	Predicting likelihood of future incidents	Analyzing past security incidents	May not account for all variables affecting incidents	Helps in better preparation and response to incidents
Data Mining Techniques	Identifying patterns in historical data	Applying data mining algorithms	Performance may degrade with large datasets	Can uncover hidden patterns and trends
Behavioral Analytics	Detecting abnormal user behavior	Analyzing user interaction with systems	Depends on the quality of behavioral models	Can detect insider threats and unusual activity
Cloud-Based Solutions	Enhancing scalability and flexibility	Leveraging cloud infrastructure	Requires strong security measures for cloud environment	Improves scalability and accessibility
Advanced Threat Modeling	Identifying potential attack vectors	Developing detailed threat models	Requires continuous updating of threat models	Helps in preemptive mitigation of threats
Network Traffic Analysis	Identifying malicious patterns	Analyzing network traffic patterns	Performance impact on network infrastructure	Helps in detecting and preventing cyber attacks
Artificial Intelligence	Enhancing automation and decision-making	Using AI algorithms for analysis	Relies on quality and quantity of data	Improves efficiency and accuracy in threat detection
Collaborative Defense	Sharing threat intelligence	Collaborating with other organizations	Requires trust among collaborating organizations	Enhances overall cyber threat defense
Endpoint Security Solutions	Protecting endpoints from threats	Deploying endpoint security solutions	May require frequent updates and maintenance	Enhances security at the endpoint level

3. Methodology

The method and technique used to study predictive analytics for cyber risks to improve security in the cyber supply chain is a thorough and organized way to collect, analyze, and make sense of data. This method is very important for making sure that the study results are true and trustworthy. The first step in the study process is to carefully read all the previous work that has been done on prediction analytics, cybersecurity, and the cyber supply chain. This review [12] of the literature helps to build a theoretical framework for the research and find important ideas, theories, and methods that are useful to the study. Next, the method includes getting information from a number of different places, such as academic papers, meeting transcripts, business reports, and case studies. Both qualitative and quantitative methods are used to look at this data and find patterns, trends, and insights that can be used to make predictions about cyber risks in the cyber supply chain.

These case studies are one of the main methods used in this research. In case studies, real-life examples of how predictive analytics has been used to make the online supply chain safer are looked at in great detail. By looking at these case studies, scholars can learn a lot about the pros, cons, and best practices of using predictive analytics in this circumstance. The use of polls and conversations is another important part of the process. Talking to experts in the field, people who work in cybersecurity and IT managers can help you understand how predictive analytics are used in the cyber supply chain right now, as well as what the challenges and trends will be in the future. An important part of the study process is analyzing the data. In order to do this, the data from literature reviews, case studies, interviews, and polls needs to be analyzed using statistics tools and methods. It is the job of the data analyst to find patterns, trends, and connections that can help answer the research questions and back up the research theories [13]. Lastly, the study technique and methods include putting together a story that makes sense based on the results of the data analysis. The study paper then presents the research results and conclusions, which are based on this story. The research approach and methods used to look into predictive analytics for cyber risks in the cyber supply chain are thorough and well-organized. Researchers can learn a lot about how predictive analytics can be used to improve security in this important area of cybersecurity by combining book reviews, case studies, interviews, polls, and data analysis methods.

4. Predictive Analytics Techniques for Threat Detection

a. *Machine learning algorithms for threat detection*

It is possible to find risks in the online supply chain with the help of machine learning (ML) programs. These programs can look through a lot of data to find trends and outliers that could point to a threat. A number of different types of machine learning methods are used to find threats, including:

- Supervised Learning: In supervised learning, the algorithm is taught on labeled data, which means that each piece of data has a name that tells it what kind of data it is (for example, normal or bad). From the training data, the program learns how to put new data points into groups based on the trends it has seen. Decision trees, random forests, and support vector machines (SVM) are all types of guided learning methods.
- Unsupervised Learning: This type of learning is used when the data doesn't have any labels on it. The program has to find trends and outliers in the data without knowing what the classes are. When unsupervised learning is used to find threats, clustering methods like k-means and hierarchical clustering are often used.
- Deep Learning: Artificial neural networks are used in deep learning, a type of machine learning, to describe complex patterns in data. Two types of deep learning models that have been used to find threats in cybersecurity are convolutional neural networks (CNNs) and recurrent neural networks (RNNs).

A lot of different kinds of data, like network traffic data, log files, and device data, can be used to teach machine learning algorithms how to find a lot of different kinds of threats, like malware infections, phishing attacks, and insider threats. You can also use these algorithms to look for new threats before they become full-blown attacks by looking at trends in data over time.

b. *Explanation of behavioral analytics and its role in detecting anomalous behavior*

Another important way to find threats in the computer supply chain is to use behavioral analytics. This method is based on looking at how people and systems act to find changes from their usual habits that could mean there is a security risk. Behavioral analytics can be used on different kinds of data, like system logs, network traffic logs, and user activity logs. One of the best things about behavioral analytics is that it can find hidden threats, which are hard to find with regular security measures. Behavioral analytics looks at trends of behavior over time to find changes in behavior that could be signs of an insider threat, like an employee getting private data outside of work hours or trying to get into systems they aren't supposed to be in. Aside from malware and hacking attempts, behavioral analytics can also be used to find other kinds of threats. Organizations can find and stop these kinds of threats before they do a lot of damage by looking at patterns of behavior that are common among them. Behavioral analytics and machine learning algorithms are strong ways to find threats in the online supply chain. These methods look for trends and oddities in data to help companies find and stop security risks before they happen. This makes the whole online supply chain safer.

c. Overview of network traffic analysis and its relevance to cyber threat detection

Network traffic analysis is an important part of cybersecurity, especially when it comes to finding cyber threats in the cyber supply chain. It includes keeping an eye on and analyzing the data bits that move through a network to find trends, oddities, and possible security threats. This summary will talk about why network traffic analysis is important and how it can help find cyber threats. We live in a world where everything is linked and businesses depend on digital networks to run. To protect private data and assets, network traffic analysis is very important. Companies can learn a lot about how people, devices, and apps behave in their network setting by keeping an eye on network data. This lets them see security risks and act on them right away, which helps stop data breaches, illegal access, and other cyberattacks.

There are a number of reasons why network data analysis is very useful for finding online threats:

- Finding Strange Patterns and Behaviors: Network traffic analysis helps businesses find strange patterns and behaviors that could be signs of a security threat. Organizations can find changes from normal behavior, like strange data transfers, shady links, or attempts to get in without permission, by setting standard traffic patterns and comparing them to real-time data.
- Identification of fraudulent behavior: Network traffic analysis helps businesses find and name fraudulent behavior happening on their networks. This includes finding signs of compromise like malware infections, hacking attacks, contact between command and control, and more. Companies can find and stop security threats before they do a lot of damage by looking at network data in real time.
- A Look at Possible Attack Vectors: Looking at network data can help you understand how cybercriminals might attack and what tools they might use. Organizations can find the methods and tools used in cyberattacks, like hack kits, malware droppers, and command and control servers, by looking at network traffic trends and packet contents. This knowledge helps businesses learn more about the strategies, tactics, and procedures (TTPs) that cybercriminals use. This lets them improve their protection and lessen the impact of future attacks.
- Forensic Analysis: Network traffic analysis is also a very important part of forensic probes that happen after a security event. By collecting and studying network traffic data, businesses can figure out what happened before a security breach, where the attack came from, and how bad the damage was. This information is very helpful for responding to incidents, going to court, and making future security steps better.

The network traffic analysis is an important part of finding cyber threats in the cyber supply chain. By keeping an eye on and studying network traffic in real time, businesses can find and stop security threats before they happen. This helps them protect their digital assets and private data. Network traffic analysis will remain an important tool for businesses that want to improve their cybersecurity and protect themselves from new threats as cyber dangers change and become more complex.

5. Integration with Cyber Security

a. Predictive analytics can be integrated into existing cyber security frameworks

Predictive analytics can be added to current protection systems to make them better at finding threats and responding to them. With this combination, businesses can use predictive analytics to find and stop online risks before they happen, in real time. There are several ways that predictive analytics can be added to security systems that are already in place:

- Better Threat Intelligence: Predictive analytics can look at a lot of threat intelligence data, like signs of capture (IOCs), threat feeds, and attack data from the past. Organizations can find patterns and trends that may point to new threats by using machine learning techniques on this data. After getting better information about threats, security controls and steps can be updated to better protect against them.
- Real-time Threat Detection: Companies can better find and stop security threats in real time by combining predictive analytics with their current security information and event management (SIEM) tools. Predictive analytics can look at network traffic, log data, and other security data sources to find strange behavior and possible security breaches. In this way, groups can move right away to stop these threats before they get worse.

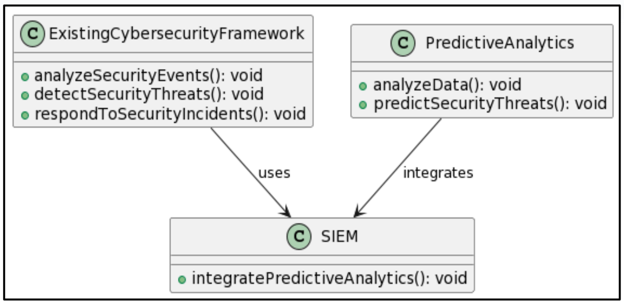
ExistingCybersecurityFramework
analyzeSecurityEvents(): void
detectSecurityThreats(): void
respondToSecurityIncidents(): void
PredictiveAnalytics
analyzeData(): void
predictSecurityThreats(): void
uses
integrates
SIEM
integratePredictiveAnalytics(): void

Figure 2: Predictive cybersecurity flow

- Behavioral Analytics: You can also use predictive analytics to make behavioral analytics models that can find strange patterns in how users act and how systems work. These models can find changes from normal behavior that could be signs of a security threat, like insider threats or accounts that have been hacked, by looking at trends of behavior over time. Adding these models to security systems that are already in place can make them better at finding and stopping these threats.
- Security Controls and Systems Predictive Maintenance: Predictive analytics can also be used to keep security controls and systems in good shape. Organizations can figure out when security controls might stop working or fail by looking at data from system performance measures, security logs, and other places. This lets companies deal with these problems before they become a threat to their safety.

Lastly, adding prediction analytics to current cybersecurity systems can make it easier to find and stop threats, give companies better security information, and let them protect themselves from cyber dangers before they happen. Organizations can improve their safety and better protect their digital assets and private information by using predictive analytics more.

b. Security information and event management (SIEM) systems and their role in predictive analytics

SIEM (Security Information and Event Management) tools are very important for adding predictive analytics to security frameworks. SIEM systems get information about security events from many places in a company's network, like network devices, computers, and apps, and then they examine that information. In real time, they help companies find and deal with security issues by tracking, warning, and reporting. In predictive analytics, SIEM systems are where all the data that needs to be analyzed is collected and processed. They can work with predictive analytics tools to use machine learning algorithms and other advanced analytics methods to look for trends and outliers in the data that could point to security risks.

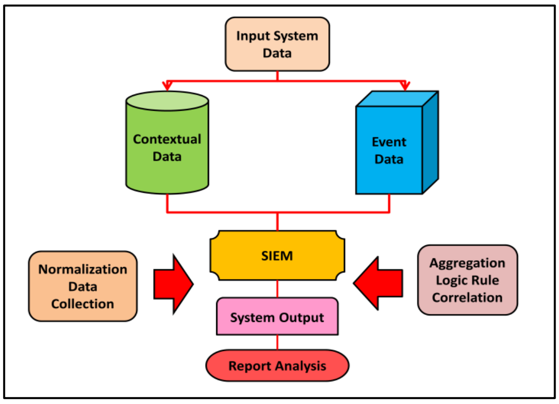

Figure 3: System architecture for SIEM

When businesses add predictive analytics to SIEM systems, they can better find and deal with new threats before they happen. SIEM systems are also very important for putting predictive analytics into practice. They give you the tools and resources you need to set up and run predictive analytics models in a real-world setting. This includes gathering data, making it normal, and finding correlations between it. It also includes giving people a way to run analytics programs and get tips based on the results. In general, SIEM systems are necessary to add predictive analytics to cybersecurity frameworks. This helps companies find and stop threats faster and protect themselves from more advanced cyber threats.

6. Applications in the Cyber Supply Chain

1. Predictive analytics can be applied to various aspects of the cyber supply chain

Different parts of the cyber supply chain can use predictive analytics to make them safer and more efficient. For instance, predictive analytics can be used in inventory management to predict demand and find the best amount of merchandise to keep on hand, which lowers the risk of running out of stock or having too much on hand. Predictive analytics can help improve operations by finding the best routes and schedules, which saves time and money. In buying, predictive analytics can look at how well suppliers are doing and guess when problems might happen, so steps can be taken ahead of time to avoid them.

2. Risk assessment and management techniques using predictive analytics

Predictive analytics can make assessing and managing risks in the cyber supply chain a lot better. Predictive analytics can figure out what risks and weaknesses might happen by looking at past data and finding trends. This helps companies decide how to best use their resources and focus their efforts to reduce risk. Predictive analytics can also give organizations real-time risk estimates that let them move quickly on new threats and lessen their effects.

3. Predictive analytics can enhance incident response capabilities within the cyber supply chain

By giving early warning signs of possible security events, predictive analytics can make incident reaction much better in the online supply chain. Predictive analytics can find strange trends and outliers that could mean there has been a security breach by looking at data from different sources like network logs, endpoint devices, and security monitors. This lets businesses react quickly and effectively to lessen the effects of cyberattacks and keep their operations running as smoothly as possible.

4. Predictive analytics in identifying and mitigating supply chain vulnerabilities

Predictive analytics can be very helpful in finding and fixing weaknesses in the supply chain. Predictive analytics can find weak spots in the supply chain, like old software or weak security controls, by looking at data from sellers, partners, and other parties. Then, this information can be used to decide which vulnerabilities need to be fixed first and to take steps to make the supply chain safer. Furthermore, prediction analytics can help businesses plan for and deal with possible problems in the supply chain, like natural disasters or political events, so that their activities don't stop. The prediction analytics could change the online supply chain by making it safer, more efficient, and more resilient. Using prediction analytics on different parts of the cyber supply chain can help businesses do a better job of assessing and managing risks, responding to incidents faster, and finding and fixing supply chain weaknesses.

7. Conclusion

Predictive analytics has a huge amount of promise to make the online supply chain safer. Organizations can effectively find and stop cyber dangers, protect their digital assets, and improve their overall security by using advanced algorithms and machine learning techniques. One of the best things about prediction analytics is that it can find new threats before they become full-on attacks. Predictive analytics looks at past data, current trends, and other factors to guess what computer dangers and weaknesses might happen. This means that companies can proactively lower these risks by doing things like fixing security holes or adding more security measures. Predictive analytics can also improve the cyber supply chain's ability to respond to incidents. Predictive analytics can help find and rank possible security events by looking at data from many sources, such as network logs, endpoint devices, and security monitors. This lets businesses react quickly and effectively to cyberattacks and lessen their effects. In general, prediction analytics is a great way to make the online supply chain safer. Organizations can effectively find and stop cyber dangers, protect their digital assets, and improve their overall security by using advanced algorithms and machine learning techniques. Predictive analytics will become more and more important in protecting the cyber supply chain and businesses from cyber dangers as they continue to rely on digital technologies to run their businesses.

References

[1] B. Debnath, A. Das, S. Das and A. Das, "Studies on Security Threats in Waste Mobile Phone Recycling Supply Chain in India," 2020 IEEE Calcutta Conference (CALCON), Kolkata, India, 2020, pp. 431-434, doi: 10.1109/CALCON49167.2020.9106531.

[2] N. Mmango and T. Gundu, "Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-6, doi: 10.1109/ICECET58911.2023.10389226.

[3] D. Liu, Y. Liu, Z. Liu, X. Zhang and X. Zhang, "Analysis and Reflection on the Situation of Industrial Information Security Ransomware Attacks," 2023 8th International Conference on Data Science in Cyberspace (DSC), Hefei, China, 2023, pp. 354-358, doi: 10.1109/DSC59305.2023.00057.

[4] S. Siddique, M. A. Haque, R. H. Rifat, R. George, K. Shujaee and K. D. Gupta, "Cyber Security Issues in the Industrial Applications of Digital Twins," 2023 IEEE Symposium Series on Computational Intelligence (SSCI), Mexico City, Mexico, 2023, pp. 873-878, doi: 10.1109/SSCI52147.2023.10371850.

[5] Sadeq Almeaibed, Saba Al-Rubaye, Antonios Tsourdos and P Nicolas, "Avdelidis. Digital twin analysis to promote safety and security in autonomous vehicles", IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 40-46, 2021.

[6] Kaznah Alshammari, Thomas Beach and Yacine Rezgui, "Cybersecurity for digital twins in the built environment: current research and future directions", Journal of Information Technology in Construction, vol. 26, pp. 159-173, 2021.

[7] Pelin Angin, Mohammad Hossein Anisi, Furkan Goksel, Ceren Gursoy and Asaf Buyukgulcu, "Agrilora: a digital twin framework for smart agriculture", J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., vol. 11, no. 4, pp. 77-96, 2020.

[8] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., & Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559

[9] Muhammad Anshari, Mohammad Nabil Almunawar and Masairol Masri, "Digital twin: financial technology's next frontier of roboadvisor", Journal of Risk and Financial Management, vol. 15, no. 4, pp. 163, 2022.

[10] Peter Augustine, "The industry use cases for the digital twin idea" in Advances in Computers volume, Elsevier, vol. 117, pp. 79-105, 2020.

[11] Maurizio Bevilacqua, Eleonora Bottani, Filippo Emanuele Ciarapica, Francesco Costantino, Luciano Di Donato, Alessandra Ferraro, Giovanni Mazzuto, Andrea Monteriu, Giorgia Nardini, Marco Ortenzi et al., "Digital twin reference model development to prevent operators' risk in process plants", Sustainability, vol. 12, no. 3, pp. 1088, 2020.

[12] Violeta Damjanovic-Behrendt, "A digital twin-based privacy enhancement mechanism for the automotive industry", 2018 International Conference on Intelligent Systems (IS), pp. 272-279, 2018.

[13] Tianhu Deng, Keren Zhang and Zuo-Jun Max Shen, "A systematic review of a digital twin city: A new pattern of urban governance toward smart cities", Journal of Management Science and Engineering, vol. 6, no. 2, pp. 125-134, 2021.