ISSN: 2321-2152

IJMECE

International Journal of modern
electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152

www.ijmece.com

Vol 13, Issue 2, 2025

The Use of Artificial Intelligence in Cyber Insurance Risk Assessment to Strengthen Cyber Defenses

[1] Mr.Ch. Surya Prakash, [2]Borra Mamatha,

[1] Associate Professor, Dept.of Master of Computer Applications

Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi, Rajahmundry, E.G. Dist. A.P. 533107.

[2] Students, Dept. of MCA, Rajamahendri Institute of Engineering & Technology, Bhoopalapatnam, Near Pidimgoyyi, Rajahmundry, E.G. Dist. A.P. 533107.

Abstract—

Several domains, such as cyber threat assessments, awareness, and compliance, have proven that artificial intelligence (AI) can effectively improve cyber security. The development of cybersecurity education, strategies, policies, and processes may also be facilitated by AI. Cyber insurance and risk assessments for cyber security are notoriously difficult to manage and quantify. A comprehensive knowledge of cybersecurity risk factors and assessment procedures is essential for cybersecurity professionals. Therefore, AI can be a useful tool for conducting a more exhaustive investigation. Through the analysis and implementation of a demonstration of how AI may assist in cybersecurity resilience, this study centers on the efficacy of AI-driven processes in improving the whole cyber security insurance life cycle. Cybersecurity risk assessment, cyber insurance, cyber security compliance, and AI-driven are some of the keywords associated with this topic.

I. INTRODUCTION

With the world going digital, safeguarding our digital assets from potential dangers and bad actors is more important than ever. Without a shadow of a doubt, cyber defense is receiving greater resources from corporations. Nevertheless, if a cyberattack succeeds, it might cause significant financial harm or even the complete collapse of a company. The already high stakes of potential legal ramifications, identity theft, and substantial financial losses are only going to rise. Even while most companies are spending money on cybersecurity knowledge, rules, and strategies, it doesn't mean there won't be attacks. Those safeguards aren't foolproof; they're becoming increasingly susceptible to social engineering attempts and technological advancements. Protecting oneself against the fallout of cyber events is possible with cyber insurance. Organizational contexts have recently been used to examine various approaches to cyber threat modeling [1]. Developed to protect people and organizations against the consequences and legal obligations stemming from cyber catastrophes, this form of insurance is also known as cyber risk insurance. Cyber insurance helps cover costs connected with effects of cyber-attacks, whether they involve data breaches, network security issues, or any other type of assault that might compromise sensitive information. Numerous applications of artificial intelligence (AI) have demonstrated fruitful outcomes. By introducing novel approaches to threat detection, prevention, and response, AI has the potential to enhance cybersecurity. To keep ahead of any new attack approaches, AI can swiftly assess trends in massive databases using machine learning algorithms. Tools driven by AI may automate cyber threat defense and fortify the overall security strategy through the use of sophisticated behavioral analysis and predictive threat identification. Artificial intelligence (AI) can provide quantified risk profiles for individuals and businesses when it comes to cyber-security risk assessment. It can process a large amount of data and come up with better premium and risk mitigation predictions. AI has the ability to examine economic trends and market data in order to forecast various investment risks [2]. This means that it may base its estimations on expected outbreaks that may be associated with a certain type of business. In this article, we'll take a look at how a pre-designed cyber insurance questionnaire may be enhanced using artificial intelligence to streamline the report generating process. The responses provide AI with significant information on data security methods, cybersecurity procedures, and risk profiles as a whole. Artificial intelligence may compare these findings to industry historical data to provide detailed reports based on data. The successful transformation of user input into insightful reports is ensured by this process. Because of this, the reporting process will be optimized more quickly and efficiently.

II. CYBERSECURITY INSURANCE AND RISK ASSESSMENT

A. Cybersecurity insurance

Protecting individuals, businesses, and institutions against financial ruin in the event of a cyberattack or other cyber-related loss is the primary goal of cybersecurity insurance [3]. Data breaches, ransomware attacks, hacking, and other cyber dangers can be costly, and cyber insurance or cyber liability insurance estimates these costs for the person or business who requests it. The cyber insurance may be tailored to match the specific needs of each firm based on their risk profile and organizational structure. Because it is dependent on the company's size, the background of its personnel, and the sector it operates in, the risk profile is a tough aspect to quantify. It can also change depending on how advanced the cybersecurity defenses are and how much protection is needed. Part B: Evaluating potential dangers

Cyber insurance companies employ several methods to evaluate risk and determine risk variables in order to set rates for organizations who want cyber insurance [2]. A thorough evaluation of the company's cybersecurity posture is often conducted, including all potential risks. In order to determine the business's total risk exposure, the insurer conducts a thorough analysis to find any weak spots or dangers [4]. As part of this evaluation, the company's data protection procedures and network security measures may be examined. The incident response and recovery plans and the security policies and procedures that have been put into place are also examined in this regard. Lastly, any potential interactions with third-party vendors and their cybersecurity procedures are reviewed, in addition to the staff training and awareness initiatives. B. The NIST RMF Model Risk management frameworks for government and companies have been addressed in many publications by the National Institute of Standards and Technology (NIST). For example, the National Institute of Standards and Technology (NIST) has developed the Risk Management Framework (RMF) to aid in the effective angement and mitigation of cybersecurity risks [5] [6]. The private sector is one of several that has embraced this methodical, multi-stage procedure. The process is comprised of seven essential phases: One must first be ready for risk management by establishing its context and priorities. Data and information systems are thereafter classified based on the gravity and sensitivity of their respective impacts. The next step is to choose and implement a set of suitable security rules. The next step is to determine how well the controls worked by conducting security assessments. The results of the risk assessment serve as the basis for obtaining authorization. Lastly, we make sure to constantly monitor and resolve any occurrences or changes. This iterative method allows organizations, particularly US government agencies, to better evaluate, reduce, and oversee cybersecurity risks while also adapting to evolving needs and dangers. The D. AI Risk Management Framework developed by the National Institute of Standards and Technology (NIST).

There has to be further thought given to the variety and complexity of AI applications in cybersecurity in order to prevent or at least lessen the impact of these dangers. Because of this, the National Institute of Standards and Technology (NIST) has just issued the AI Risk Management Framework (AI RMF) [7] to aid businesses and people in efficiently and effectively managing the risks connected with AI. In order to help businesses adjust to these risks, this framework defines a procedure that is both flexible and iterative. Put another way, this structure clarifies how to control the dangers that come with applying AI systems to various fields.

.

III. CYBERSECURITY INSURANCE USING AI

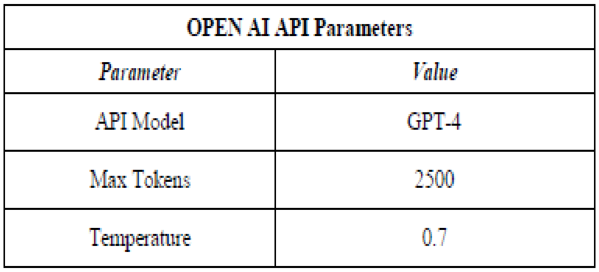
A. Objective.

To facilitate the integration of AI capabilities into many domains, the majority of AI systems provide Application Programming Interfaces (APIs). Programmable scripts that may be executed automatically are described in these APIs as a means to interact with AI models. As a result, different modules will be able to make advantage of AI capabilities. Cyber security evaluations and analyses may be easily generated with the use of artificial intelligence (AI) skills, which is especially useful given the complexity of providing cyber insurance. [8]

Customers are asked to complete a series of short, well-structured questions by means of a designed application that implements the suggested technique. To ensure that the insurance adequately addresses the organization's unique cybersecurity needs, the form questions and responses are processed into the ChatGPT API for a precise evaluation. In addition, the API is utilized to accurately explain each component and its queries, ensuring that the client or their representative comprehends and completes the form to the best of their ability. Section B: Approach.

Asking the customer to fill out a lengthy questionnaire is the first step in getting a cybersecurity insurance evaluation. The questionnaire is an organized method of collecting crucial data on the client's company processes, IT setup, and data protection protocols. Organizational cyber risk exposure, current security procedures, incident response strategies, and breach incidences in the past are some of the subjects covered in the questionnaire. The insurance company may gauge the degree of cybersecurity risk from the consumers' replies and then design a policy that fits their needs. Accurate and effective coverage against possible attacks and breaches may be achieved by taking the time to understand the client's individual needs and tailoring the insurance policy to their unique cybersecurity requirements. C. Questionnaire on cybersecurity. Divided into four sections, the questionnaire consists of a set of questions. Questions concerning the organization's assets, network, website, content, technological products, and media activities make up the first part of the survey. It is essential to have a thorough grasp of these aspects in order to determine the overall cybersecurity risk profile. The media-related activities of an organization, the complexity of its network architecture, the value and sensitivity of its assets, the content on its website, and the products it employs for technology all contribute to the potential vulnerabilities and hazards that the business faces. This section covers the following topics: • Assets: Private and business data, as well as critical information. • Devices, Software, and Related Services Infrastructure, servers, and the security of te network • Online Presence: Content and Media Operations on the Web • Media - Actions, Reviews, and Approval by Lawyers • Backups, Log Monitoring, and Security Configuration Controls Rules for protecting sensitive data, maintaining operations in the event of a disaster, and meeting regulatory requirements are all addressed in Section 2. An organization's dedication to security, preparedness to deal with interruptions, and compliance with regulatory obligations are all reflected in this crucial component. Questions on the following are included in this section: • Policy on Information Security • Business Continuity and Recovery Timeframes • A policy on privacy; • A plan for when an incident occurs; • A strategy for ensuring compliance and governance. Data loss prevention (DLP) includes measures such as encryption, filtration, mitigation, firewalls, and separation. Service providers, training, and awareness are the topics covered in depth in the third portion of the questionnaire. The cyber insurance plan of the firm relies heavily on this part. Insurers take the security standards of service providers seriously because of the access they have to an organization's data and systems. To avoid or at least lessen the impact of cyber events, training and awareness are equally important. Social engineering assaults account for the vast majority of cyberattacks, according to studies. Security breaches are less likely to occur when employees are taught on best practices for cybersecurity. Cloud-based providers, non-IT service providers, providers of IT services, and training and awareness Security, privacy, and previous claims and events are the main topics of the last part. Cyber insurance is based on past security and privacy incidents. Insurers can assess risk profiles and claims histories by reviewing data on historical events, claims, and reactions. To fully grasp the ins and outs of your cyber insurance policy, it is crucial to have a firm grasp of this subject. Only then can you assess your organization's readiness to handle security and privacy concerns. Unauthorized disclosure, improper collection, storage, use, or processing, and claims arising from prior regulations are all examples of security and privacy claims. Criminal: Transactions, Authentication, and Next-Level Approval • Past Claims Experience or Incidents That Might Give Rise to a Claim The majority of the 208 items on the survey are easy multiple-choice questions. A risk assessment will be prepared when the customer's replies are processed to ChatGPT via API. D. The Application of AI. One goal of the AI integration module is to decipher the customer's queries and answers; another is to compile a list of specific risk assessments. The prompt and data are sent to the Open AI API when the two datasets are formed. The module communicates with Open AI 4.0 via an Integration RESTful interface and creates the pre-defined risk factor fields automatically. Table 1 displays the parameters that are required to communicate with the API. The next step is to reorganize the output such that it contains the metrics required to calculate the insurance quote.

TABLE I. OPEN AI API PARAMETERS



OPEN AI API Parameters	
Parameter	*Value*
API Model	GPT-4
Max Tokens	2500
Temperature	0.7

IV. DEMONSTRATION AND RESULTS.

Applying the proposed module to a list of 100 customer answer samples and then communicating the material to OpenAI's most powerful API, GPT-4, to produce structured content for different controls is how the module is presented. All of the necessary metrics were produced. Analyses powered by AI can efficiently and accurately gauge cyber dangers. In addition, it compiles a set of suitable cybersecurity measures that may be utilized for insurance purposes. In the ever-changing world of cybersecurity, the data gathered is based on a data-driven and dynamic approach to risk management. Upon submission of the questions and their responses to the AI API, the subsequent risk assessments were produced. o The total amount of potential dangers and risks that have been recognized. o Risks are categorized. • Danger Level and Its Effects: o Calculation of Possible Monetary Loss o The monetary effect on operations of each risk. o An indicator of how serious an adverse occurrence will be. The chance, in percentage or frequency, of each danger happening is known as the risk probability. · Incidents and losses that have already occurred, with a monetary value assigned to the frequency and seriousness of such risks. • Risk Exposure: o All the hazards that a person is exposed to in total, as measured by the sum of their individual impacts or other pertinent metrics. Examining past data to spot patterns in the frequency, likelihood, and severity of risks is what "risk trends" are all about. • Mitigation of Risk: o The efficacy of current mitigation strategies, often conveyed as a reduction in risk exposure percentage. • Conformity: o Measuring conformity to applicable rules, norms, and recommendations.
o The total amount and frequency of prior insurance claims pertaining to risks. Paying insurance premiums in the past is one example of a premium history.

V. CONCLUSION

Our research here focused on the ways AI might improve cyber insurance risk assessment and cybersecurity resilience. In order to shift the risk of monetary losses and damages, several firms have recently shifted to cyber insurance. Methods powered by artificial intelligence (AI) are crucial to this procedure because they allow for more thorough examination of cybersecurity risk factors and the creation of precise, individualised insurance policies. To help firms better understand their risk exposure, discover vulnerabilities, and strengthen their cybersecurity defenses, this study use AI to analyze data from a well-structured questionnaire. Artificial intelligence (AI) may also help with the building of a customized insurance quotation that meets the unique demands of a company.

REFERENCES

[1] L. Pavlik, "Identifying and Modeling the Impact of Cyber Threats in theField of Cyber Risk Insurance," *2018 5th International Conference on Mathematics and Computers in Sciences and Industry (MCSI)*, Corfu,Greece, 2018, pp. 118-121, doi: 10.1109/MCSI.2018.00036.

[2] M. Francesca Carfora and A. Orlando, "Quantile based risk measures incyber security," *2019 International Conference on Cyber SituationalAwareness, Data Analytics And Assessment (Cyber SA)*, Oxford, UK,2019, pp. 1-4, doi: 10.1109/CyberSA.2019.8899431.

[3] R. R. Zgraggen, "Cyber Security Supervision in the Insurance Sector:Smart Contracts and Chosen Issues," *2019 International Conference onCyber Security and Protection of Digital Services (Cyber Security)*,Oxford, UK, 2019, pp. 1-4, doi: 10.1109/CyberSecPODS.2019.8885404.

[4] C. Lin, F. Liu, L. Zhang, G. Li, C. Chen and Z. Bie, "An online datadrivenrisk assessment method for resilient distribution systems," in*CPSS Transactions on Power Electronics and Applications*, vol. 6, no.2, pp. 136-144, June 2021, doi: 10.24295/CPSSTPEA.2021.00012.

[5] A. Gui, R. Kristanto, H. Haron and E. Adrian, "Information TechnologyRisk Measurement Using NIST (Case Study at Pt. Pintraco)," *2010Second International Conference on Advances in Computing, Control,and Telecommunication Technologies*, Jakarta, Indonesia, 2010, pp.191-194, doi: 10.1109/ACT.2010.57.

[6] W. Matsuda, M. Fujimoto, T. Aoyama and T. Mitsunaga, "CyberSecurity Risk Assessment on Industry 4.0 using ICS testbed with AI andCloud," *2019 IEEE Conference on Application, Information andNetwork Security (AINS)*, Pulau Pinang, Malaysia, 2019, pp. 54-59, doi:10.1109/AINS47559.2019.8968698.

[7] National Institute of Standards and Technology. "AI Risk ManagementFramework." NIST January 26, 2023. Available online:https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[8] J. C. Haass, "Cyber Threat Intelligence and Machine Learning," *2022Fourth International Conference on Transdisciplinary AI (TransAI)*,Laguna Hills, CA, USA, 2022, pp. 156-159, doi:10.1109/TransAI54797.2022.00033.

[9] G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano and T.J. Tokola, "Poster: The Need for a Collaborative Approach to CyberSecurity Education," 2021 IEEE European Symposium on Security andPrivacy (EuroS&P), Vienna, Austria,

2021, pp. 719-721, doi:10.1109/EuroSP51992.2021.00058.

[10] M. Neumann, M. Rauschenberger and E. -M. Schön, "“We Need to TalkAbout ChatGPT”: The Future of AI and Higher Education," *2023 IEEE/ACM 5th International Workshop on Software EngineeringEducation for the Next Generation (SEENG)*, Melbourne, Australia, 2023, pp. 29-32, doi: 10.1109/SEENG59157.2023.00010.

[11] L. Li, W. He, L. Xu, A. Ivan, M. Anwar and X. Yuan, "Does ExplicitInformation Security Policy Affect Employees' Cyber SecurityBehavior? A Pilot Study," 2014 Enterprise Systems Conference,Shanghai, China, 2014, pp. 169-173, doi: 10.1109/ES.2014.66.

[12] V. Sundararajan, A. Ghodousi and J. E. Dietz, "The Most CommonControl Deficiencies in CMMC non-compliant DoD contractors," *2022IEEE International Symposium on Technologies for Homeland Security(HST)*, Boston, MA, USA, 2022, pp. 1-7, doi:10.1109/HST56032.2022.10025445.

[13] P. P. Roy, "A High-Level Comparison between the NIST Cyber SecurityFramework and the ISO 27001 Information Security Standard," 2020National Conference on Emerging Trends on Sustainable Technologyand Engineering Applications (NCETSTEA), Durgapur, India, 2020, pp.1-3, doi: 10.1109/NCETSTEA48365.2020.9119914.