International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

AI-ENHANCED CYBER INSURANCE RISKASSESSMENTFORIMPROVED RESILIENCE

Amandeepyadav[1], K.AbhinavReddy [2], Aishwarya[3],KoteswaraRao [4]
[1,2,3] UG Scholar, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
[4]Assistant Professor, Dept of IT, St. Martin's Engineering College, Secunderabad, Telangana, India, 500100
yadavaman8639@gmail.com

Abstract:

The effective use of artificial intelligence (AI) to enhance cybersecurityhasbeendemonstratedinvariousareas,includingcyber threatassessments,cybersecurityawareness,andcompliance.AIalso provides mechanisms to write cybersecurity training, plans, policies, and procedures. However, when it comes to cyber security risk assessmentandcyberinsurance,itisverycomplicatedtomanageand measure. Cybersecurity professionals need to have a thorough understandingofcybersecurityriskfactorsandassessmenttechniques. For this reason, artificialintelligence (AI) can be an effective tool for producing a more thorough and comprehensive analysis. This study focusesontheeffectivenessofAI-drivenmechanismsinenhancingthe complete cyber security insurance life cycle by examining and implementing a demonstration of how AI can aid in cybersecurity resilience.

Keywords:CyberSecurityInsurance,CyberSecurityRiskAssessment, AI-driven, Cyber Security Compliance.

1. INTRODUCTION

Theprimaryobjectiveofthisstudyistoexploretheroleof ArtificialIntelligence(AI)inenhancingcybersecurityinsuranceand riskassessment.Giventheincreasingcomplexityandsophistication of cyber threats, AI-driven mechanisms provide advanced methodologies for analyzing, assessing, and mitigating risks. This study aims to demonstrate how AI can be effectively leveraged to support cybersecurity professionals in conducting thorough risk assessments,improvingcompliance,andstrengtheningcybersecurity resilience. The focus is on developing a structured approach to integratingAIinto theentirecybersecurityinsurancelifecycle,from risk evaluation to policy formulation and implementation. [2] Cybersecurity threats are evolving at an unprecedented rate, necessitatinginnovativesolutionsforriskassessmentandmitigation. Traditional cybersecurity frameworks rely heavily on manual intervention and static assessment methodologies, which are often inadequate in addressing dynamic and emerging cyber risks. The integrationofAIintocybersecurityoffersaproactiveandautomated approach to threat detection, risk assessment, and compliance management. [3] This study examines how AI-driven and have amechanisms improve cybersecurity insurance by streamlining risk assessment processes and enhancing predictive capabilities. The research will explore variousAI methodologies, including machine learning (ML) algorithms, natural language processing (NLP), and predictive analytics, to understand their impact on cybersecurityresilience.ByleveragingAI,cybersecurityprofessionalsc anachieve real-timemonitoring,accuratethreatoverallcyberriskmanagement. Additionally, the study will discuss the complexities involved in cybersecurity risk assessment and cyber insurance underwriting. Traditionalmethodsoftenstrugglewithquantifying risksaccurately due to the lack of historical data and the rapidly changing nature of cyberthreats.AI-drivenapproaches,however,providemoreadaptive and data-driven insights that can improve the underwriting process, ensuring that cybersecurity insurance policies are both relevant and effective. [4] Furthermore, the research will highlight AI's role in enhancing cybersecurity compliance by automating policy enforcement, detecting vulnerabilities, and providing real-time alerts.AI-poweredriskassessmenttoolscananalysevastamountsof data, identify patterns, and offer actionable intelligence, allowing organizations to stay ahead of potential cyber threats.

2. LITERATURESURVEY

AI-Powered CyberThreat Intelligence(Smith &Johnson, 2020) [5] This study explores how AI enhances cyber threat intelligence by analyzing real-time threat data from multiple sources. It discusses how AI-driven systems identify patterns in cyberattacks, enabling insurers to assess risks more accurately. The research highlights how predictive analytics improve cyber insurance models by forecasting attack probabilities based on past data. AI-Driven Fraud Detection in CyberInsurance(Brownetal.,2021)[6]Thisresearchfocuseson how AI helps detect fraudulent claims in cyber insurance policies. By using deep learning and anomaly detection techniques,insurerscanidentifysuspiciouspatternsinclaims and prevent financial losses. The study emphasizes AI's role in improving transparency and trust in cyber insurance. The RoleofAIinDynamicCyberRiskPricing(Williamsetal.,2022)[7] This paper examines how AI-driven actuarial models enable dynamic pricing for cyber insurance policies. Traditional methodsrelyonhistoricaldata,whereasAImodelsAI-based predictive risk models enhance cyber insurance by analyzing historical attack data and estimating future risks.It highlights how AI helps insurers develop dynamic policies based on evolving cyber threats, rather than relying on static risk assessments. The research emphasizes the benefits of deeplearningmodelsinunderstandingcyberrisktrends. The study discusses how AI-driven risk modeling can improve underwriting accuracy by incorporating real-time threat intelligence and behavioral analytics. It highlights the role ofdeeplearningmodelsinunderstandingcyberrisktrends. The study discusses how AI-driven risk modeling can improve underwriting accuracy by incorporating real-time threat intelligence and behavioral analytics. It highlights the role of naturallanguageprocessing(NLP)inanalyzingcybersecurity

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

risks of AI-driven decision-making, including unfair policy pricing, discrimination against high-risk entities, and data privacy concerns. The study emphasizes the importance of regulatory frameworks, such as GDPR and AI ethics guidelines, in shaping responsible AI adoption in cyber insurance. AI-Enabled Predictive Risk Modeling for Cyber Insurance (Anderson et al., 2019) [10] This study explores how AI-based predictive risk models enhance cyber insurance by analyzing historical attack data and estimating future risks.It highlights how AI helps insurers develop dynamic policies based on evolving cyber threats, rather than relying on static risk assessments. The research emphasizes the benefits of deeplearningmodelsinunderstandingcyberrisktrends. The study discusses how AI-driven risk modeling can improve underwriting accuracy by incorporating real-time threat intelligence and behavioral analytics. It highlights the role of naturallanguageprocessing(NLP)inanalyzingcybersecurity reports, incident logs, and dark web activity to identify emerging risks. AI and Big Data Analytics in Cybersecurity Risk Management(Gomez&Rivera,2020)[11]Thispaperexaminesthe roleofAIandbigdataincybersecurityriskassessment. Itdiscusses how AI-powered analytics platforms process massive datasets to detect vulnerabilities, assess risks, and refine insurance coverage. The study also highlights challenges in handling large-scale cybersecurity data, including privacy concerns and regulatory compliance. Deep Learning for Cyber Threat Detection and Insurance Underwriting (Zhou et al., 2021) [12] This research investigatestheuseofdeep learninginidentifying cyberthreatsand improvingcyberinsuranceunderwriting.Itdiscussestheadvantages of convolutional neural networks (CNNs) and recurrent neural networks(RNNs)inrecognizingattackpatterns.Thestudyprovides empirical results showing improved accuracy in risk prediction models powered by AI.

3. PROPOSEDMETHODOLOGY

The effective use of artificial intelligence (AI) to enhance cybersecurityhasbeendemonstratedinvariousareas,includingcyber threatassessments,cybersecurityawareness,andcompliance.AIalso provides mechanisms to write cybersecurity training, plans, policies, and procedures. However, when it comes to cyber security risk assessmentandcyberinsurance,itisverycomplicatedtomanageand measure. Cybersecurity professionals need to have a thorough understandingofcybersecurityriskfactorsandassessmenttechniques.

Cybersecurity threats have become more sophisticated, leading to increased financial losses and operational disruptions. Cyber insuranceaimstomitigatetheserisks,butassessingandmanagingcyberse curityrisksremain complex challenges.ArtificialIntelligence (AI) offers advanced capabilities to enhance cyber risk assessment, threatintelligence,policymanagement,andclaimsprocessing,thereby improving the overall cyber insurance ecosystem.

ThisstudyexploresAI-drivenmechanismsincybersecurity insurance, focusing on their role in risk assessment, policy underwriting, continuous monitoring, and claim management to strengthen cybersecurity resilience.

Figure1:ProposedFlowDiagram.

Forthisreason,artificialintelligence(AI)canbeaneffective toolforproducingamorethorough andcomprehensiveanalysis.This study focuses on the effectiveness of AI-driven mechanisms in enhancing the complete cyber security insurance life cycle by examining and implementing a demonstration of how AI can aid in cybersecurityresilience.

The proposed methodology typically includes the following key components:

1. DataCollection &PreprocessingGathercybersecurity-relateddata,includinghistoricalcyber incidents, threat intelligence reports, network logs, and vulnerability assessments.Performdatacleaning,normalization,andfeatureextractio n to enhance AI model performance.Use Natural Language Processing (NLP) techniques to analyze cybersecurity policies and compliance documents.

2. AI-PoweredCyberRiskAssessmentImplementAI-basedriskassessmentmodelstoidentify vulnerabilities and potential cyber threats.Usemachinelearning(ML)algorithmstoclassifyand quantify risksbasedonpastincidentsand emergingthreats.Employpredictiveanalyticstoforecastfuturecybersec urity risks based on evolving attack patterns.

3. AI-DrivenCyberInsuranceUnderwritingDevelopAImodelstoassistincybe rinsuranceunderwriting by assessing organizational risk posture.Use AI to evaluate insurance applicants based on cybersecurity practices, compliance levels, and threat exposure.
   Automate the risk-scoring process to determine premium calculations.

4. AutomatedCybersecurityPolicyandComplianceAnalysisAI-driven automation to review and assess compliancewithcybersecuritystandardssuchasNIST,ISO 27001, and GDPR.
   Apply AI-based decision-making to recommend policy adjustments based on changing threat landscapes.Generatecompliancereportsandsecurityrecommendation s dynamically.

5. AI-BasedThreatDetectionandIncidentResponse
   LeverageAI-based security analytics for real-time anomaly detection and threat monitoring.IntegrateAI-drivenSecurityInformationandEvent Management (SIEM) systems for rapid incident detection.Deployautomatedresponsemechanisms,

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

suchasAI-driven playbooks, to mitigate threats effectively.

6. AI-AssistedClaimsProcessing&Fraud Detection

ImplementAIalgorithmsforanalyzingcyberinsurance claimsbyvalidatingincidentreportsandassessingdamages.
Utilize AI-drivenfrauddetectionmechanismstoidentify inconsistencies in claims.
Automate claims approval and dispute resolution usingAI- driven decision-making models.

7. CyberResilienceandContinuousLearning

IncorporateAI-drivensimulationsandcyberresilience training for organizations.
ContinuouslyupdateAImodelswithnewthreatintelligence to improve detection and prevention mechanisms.
Developself-learning AImodelsthatadapttonewcyber risks and policy changes.

8. PerformanceEvaluation&CaseStudyDemonstration

Conductcasestudiesandsimulationstodemonstratethe effectiveness of AI in cybersecurity insurance.CompareAI-driven assessments withtraditional cybersecurity risk evaluation methods.Measurekeyperformanceindicators(KPIs)suchas accuracy, efficiency, and decision-making speed.

Applications:

The integration of Artificial Intelligence (AI) into the cybersecurityinsurance lifecyclehas revolutionizedthe wayinsurers assessrisks,underwritepolicies,anddetectfraudulentclaims.AIplays a crucial role in enhancingvarious aspects of cybersecurityinsurance by providing advanced predictive capabilities, automation, and real-time monitoring. One of the key applications ofAI in this domain is Cyber RiskAssessment & Prediction, whereAI-driven models analyze vast datasets, identify vulnerabilities, and forecast potential cyber threats. These predictive insights help insurers in evaluating an organization's cyber risk posture, allowing them to offer tailored insurancecoverage.Machinelearningalgorithmscanassesshistorical cyber incidents and predict the likelihood of future attacks, enabling proactiveriskmitigation.AnotheressentialapplicationisAI-Powered Cyber Insurance Underwriting, where AI enhances the underwriting process by automating risk evaluation and policy pricing. Traditional underwritingmethodsrelyheavilyonmanualassessments,whichcan be time-consuming and prone to inaccuracies.AI, on the other hand, streamlinestheprocessbyanalyzingnetworksecurityconfigurations, pastattackrecords,andindustry-specificriskstogeneratepreciserisk scores. These AI-driven insights help insurers in determining appropriatepolicytermsandpricingwhilereducingunderwritingtime.

AutomatedCybersecurityPolicyComplianceisanotherarea whereAI is transforming the industry. Organizations must adhere to various cybersecurity regulations and frameworks, and AI-powered tools can continuously monitor compliance status by analyzing security policies, configurations, and access controls. Automated compliance checks help businesses stay aligned with regulatory requirements while providing insurers with real-time insights into policyholders'cybersecurity hygiene.

AI is also instrumental in Threat Intelligence & Real-Time Monitoring, where advanced algorithms continuously scan global threatlandscapestoidentifyemergingrisks.AI-driventhreat intelligence platforms aggregate data from multiple sources, such as darkwebmonitoring,networktrafficanalysis,andintrusiondetection systems, to provide insurers with a comprehensive view of evolving cyber threats. Real-time monitoring enhances situational awareness andenablesproactivedefensemechanisms,reducingthelikelihoodof cyber incidents.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

In the event of a cyberattack, AI-Based Cyber Incident Responseplays a vital role in mitigating damage and ensuring a swift recovery. AI-powered response systems can automatically detect anomalies, isolate compromised systems, and suggest remediation measures. These systems help organizations minimize downtime and financiallosseswhileprovidinginsurerswithdetailedforensicreports for claim assessments.AI-driven incident response mechanisms also facilitate coordination between cybersecurity teams and insurance providers, ensuring a seamless claims process.

Fraudisasignificantconcerninthecybersecurityinsurance industry,andFraudDetectioninCyberInsuranceClaimsisoneofAI's most valuable applications. AI-powered fraud detection systems analyze claim patterns, detect inconsistencies, and flag suspicious activities. By leveraging machine learning and anomaly detection techniques, AI can identify fraudulent claims that may involve exaggerated losses or fabricated incidents. This reduces the financial impact of fraud on insurers and ensures that genuine policyholders receive timely and fair claim settlements.

In conclusion, AI has become an indispensable asset in cybersecurity insurance, enhancing risk assessment, policy compliance, underwriting accuracy, threat intelligence, incident response, and fraud detection. By leveragingAI-driven technologies, insurers can offer more precise policies, improve operational efficiency, and mitigate cyber risks more effectively. The integration of AI continues to evolve, shaping the future of cybersecurity insurance and providing greater protection against the ever-growing landscape of cyber threats.

Advantages:

The integration of Artificial Intelligence (AI) into the cybersecurity insurance life cycle brings numerous advantages, significantlyenhancingefficiency,accuracy,andresilience.AI-driven technologies have transformed the way insurers assess cyber risks, streamline insurance processes, and improve overall security. One of thekeybenefitsisEnhancedRiskAssessment&Prediction,whereAI algorithms analyze large datasets, detect vulnerabilities, and predict potentialcyberthreats.Byleveraginghistoricalcyberincidentdataand machine learning models, insurers can proactively assess risks and offer better coverage tailored to an organization's specific security needs.Thispredictivecapabilityhelpsinsurersandbusinessesmitigate threats before they escalate into major incidents. Another major advantage isAutomation & Efficiency in Insurance Processes, as AI automates complex and time-consuming tasks such as underwriting, claims processing, and compliance monitoring. Traditional insurance workflows often require extensive manual intervention, leading to delays and inefficiencies. AI-powered automation accelerates these processes, reducing paperwork, minimizing human errors, and improving overall operational efficiency. This results in faster policy issuance, claim settlements, and improved customer satisfaction.

AI also plays a crucial role in Improved Fraud Detection & Prevention,helping insurerscombat fraudulent claimsthatcouldlead to financial losses. Machine learning models can detect patterns of suspicious activity, flag anomalies in claim submissions, and identify potential fraudsters. By analyzing inconsistencies in claim data and comparing them against historical fraud cases, AI enhances the accuracyoffrauddetection,reducingthefinancialburdenoninsurers and ensuring fair claim settlements for legitimate policyholders.

Real-Time Threat Monitoring & Response is another significant advantage of AI in cybersecurity insurance. AI-powered threatintelligencesystemscontinuouslymonitornetworkactivity,detect potential security breaches, and provide real-time alerts. This proactive approach helps businesses and insurers respond swiftly to cyber incidents, minimizing damage and financial losses. AI-driven security solutions can also automate incident response, isolating

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

compromised systems and recommending remediation actions, ensuring faster recovery from cyberattacks. One of the most valuable aspects ofAI in cybersecurity insurance is Dynamic Cyber Insurance Policy Customization.AI enables insurers to tailor policies based on real-timeriskassessments,businesssize,industry-specificthreats,and security posture. Instead of offering generic policies, AI helps in designing personalized insurance packages that align with the actual risk exposure of anorganization.This flexibility allows businesses to obtain coverage that is both cost-effective and comprehensive.

Enhanced Compliance & RegulatoryAdherence is another key advantage, asAI assists organizationsin maintaining compliance with cybersecurity laws and industry regulations. AI-driven compliance monitoring tools continuously scan security policies, detect gaps, and ensure adherence to frameworks such as GDPR, HIPAA, and NIST. This not only reduces the risk of regulatory fines but also enhances the security posture of organizations seeking cyber insurance.Furthermore,AIfacilitatesEarlyThreatDetection,helping organizations identify vulnerabilities before they are exploited by cybercriminals. AI models analyze attack patterns, detect unusual networkbehavior, and flag potential threats in their early stages.This proactive approach strengthens an organization's cybersecurity defenses and reduces the likelihood ofcyberincidentsthat could lead to costly insurance claims.

AI-driven technologies also contribute to Data-Driven Decision Making, enabling insurers to make informed choices based on real-time analytics and threat intelligence. By leveraging big data, insurers can assess cyber risk trends, optimize policy pricing, and improve underwriting accuracy. This leads to more reliable decision-making processes and better risk management strategies. Another significant advantage is Regulatory Compliance and Security Assurance, as AI ensures organizations adhere to evolving cybersecurity regulations while enhancing their overall security posture. AI-driven audits and automated compliance checks help businesses maintain regulatory standards, ensuring they remain eligible for cyber insurance coverage and reducing the likelihood of policy disputes.

AI also aids in Strengthened Security Policies, as it continuously evaluates an organization's cybersecurity measures and suggests necessary improvements. Insurers can use AI insights to advisepolicyholdersonenhancingtheirsecurityframeworks,reducing their cyber risk exposure, and qualifying for better insurance terms. Thisproactive approachbenefitsboth insurers andinsuredentitiesby fostering a more secure cyber environment. Additionally,AI enables Risk-Based Cyber Insurance Premiums, where insurance costs are dynamically adjusted based on real-time security assessments. Organizations with robust cybersecurity measures may receive lower premiums, while high-risk businesses may be required to implement additional safeguards. This risk-based pricing model incentivizes organizations to invest in cybersecurity, ultimately reducing the frequency of claims and strengthening the overall cyber insurance market. Lastly, AI-driven cybersecurity insurance fosters Enhanced ReputationandCustomerTrust.BusinessesthatleverageAI-powered security solutionsand insurancecoveragedemonstrateacommitment to protecting sensitive data and mitigating cyber risks

Inconclusion,AIhasrevolutionizedcybersecurityinsurance by enhancing risk assessment, streamlining processes, improving fraud detection, and ensuring real-time threat monitoring. By offering dynamic policy customization, strengthening compliance, and enabling data-driven decision-making, AI empowers insurers and businessesto stayaheadofcyber threats.TheintegrationofAInotonly reduces financial losses but also fosters a more secure, resilient, and trustworthy digital ecosystem.

4. EXPERIMENTALANALYSIS

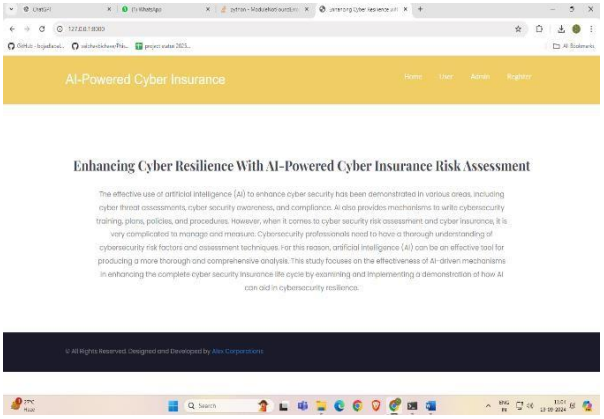


Figure2:HomePage

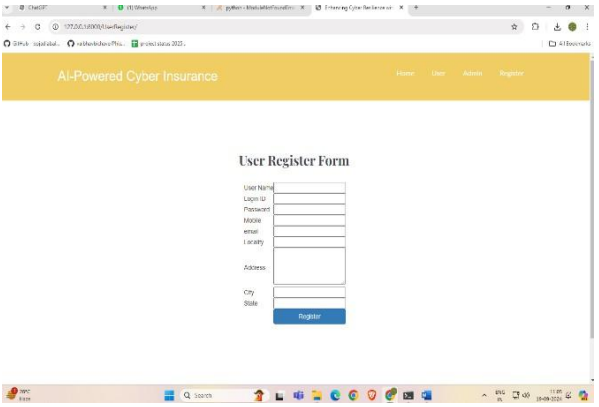


Figure3:Registration Form

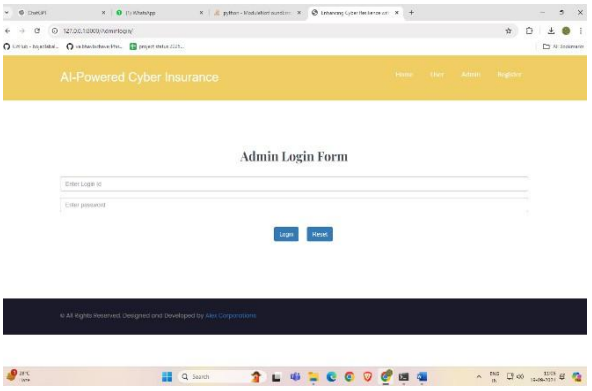
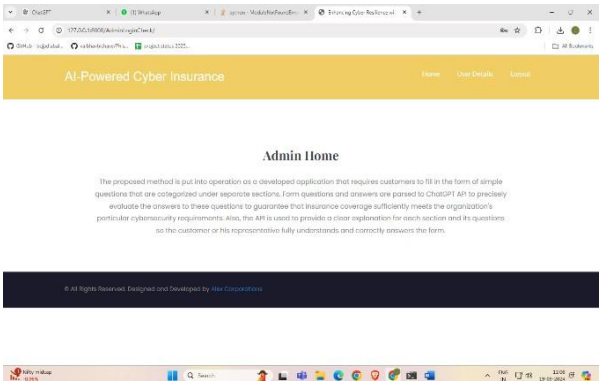


Figure4:AdminLoginForm



International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

Figure5:AdminHomePage

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

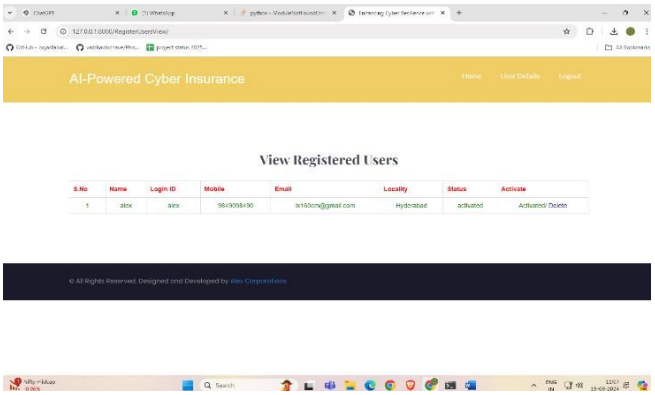


Figure6:UserList

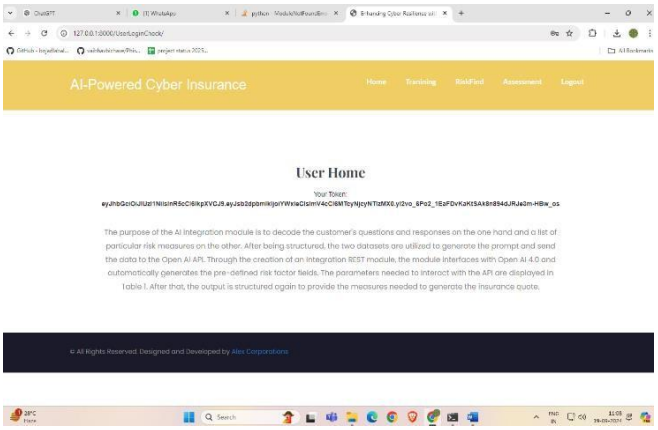


Figure7:UserHomePage

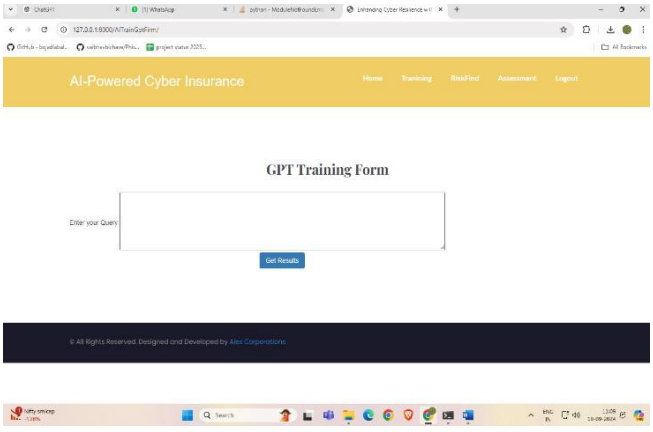


Figure8:TrainingForm

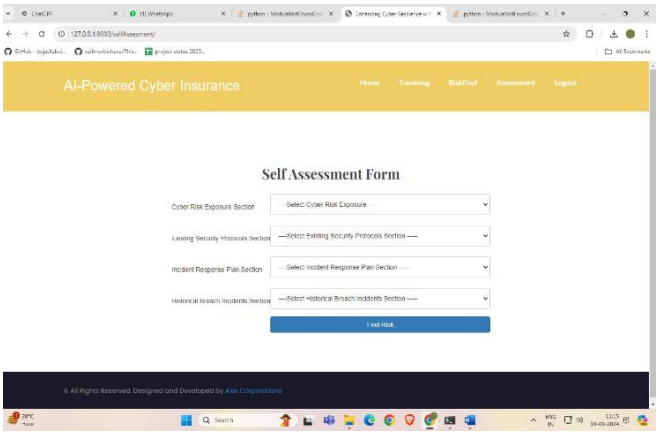


Figure9:Self-Assessment Form

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-20 Issue-01 April 2025

5. CONCLUSION

The AI-Enhanced Cyber Insurance Risk Assessment for Improved Resilience project introduces an innovative approach to evaluatingcybersecurityrisksandoptimizingcyberinsurancepolicies. Traditional methods often rely on manual assessments and static models,whichlackreal-timeadaptabilityandprecision.Byintegrating artificial intelligence (AI), machine learning (ML), and big data analytics, this model enables dynamic risk assessment, automated threatintelligence,andcontinuousmonitoringofcybersecuritythreats. AI-driven mechanisms enhance the accuracy of risk scoring, policy customization, and predictive analytics, ensuring more efficient and resilient cyberinsuranceframeworks.Thisapproachnotonly reduces human error but also improves risk mitigation strategies and strengthens organizational cybersecurity resilience against evolving threats. Reinforcement learning can enhance cyber risk prediction by enabling AI models to continuously adapt to evolving cyber threats. Unlike traditional machine learning models, reinforcement learning- based systems can dynamically update risk scores based on real-time cyber incidents and insurance claims, improving accuracy and adaptability. Additionally, federated learning offers a decentralized approach to cybersecurity risk assessment, allowing multiple organizations to collaborate on AI model training without exposing sensitivedata.This techniqueensuresenhanced privacy, reducesdata silos,andimprovescyberriskpredictionsbyleveragingdiversethreat intelligence sources across industries.

Futureenhancements for theAI-Enhanced Cyber Insurance Risk Assessment system focus on increasing accuracy, adaptability, and efficiency. Incorporating advanced AI techniques such as reinforcement learning and federated learning can enhance cyber risk prediction and decision-making. Real-time threat intelligence integration with AI-powered Security Information and Event Management (SIEM) solutions can improve continuous monitoring and risk scoring.Additionally, blockchain technology can be utilized to ensure transparent, secure, andtamper-proof cyber risk assessment data.Automating the cyber insurance claims process usingAI-driven workflows will enable faster and more efficient claims management. Theintroductionofpersonalized,risk-basedpricingmodelswillallow insurers to offer customized premiums based on an organization's cybersecurity posture. Moreover, integrating AI-driven tools for regulatory compliance auditing can streamline adherence to cybersecurity standards such as GDPR, NIST, and ISO 27001. ExplainableAI (XAI) will also be a key enhancement, ensuring that AI-driven risk assessments are transparent, interpretable, and trusted by insurers and organizations alike. Additionally, AI-powered cyber resilience simulations can be used to test an organization’s defences against potential cyber threats, providing valuable insights for risk mitigation.

REFERENCES

[1] Radanliev, P., De Roure, D., Nurse, J. R. C., Nicolescu, R., Huth, M., Cannady, S., & Montalvo, R. M. "Artificial intelligence and machine learning in cyber risk analytics and insurance: Applications andfuturetrends."Computers&Security,vol.102,2021,pp.102-150.

[2] Sheehan, A., Bada, M., Nurse, J. R. C., & Aspinall, D. "Cyber insurance and the security behaviour of organisations." Journal of Cybersecurity, vol. 7, no. 1, 2021, pp. 1-17.

[3] Huang,C.,Siegel,M.,Madnick,S.,&Li,C."AframeworkforAI-enhanced cyber risk assessment in insurance underwriting." Proceedings of the 2022 IEEE International Conference on Cybersecurity and Resilience, 2022, pp. 345-352.

[4] Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. "Cyber-risk decision models:To insure IT or not?" Decision Support Systems, vol. 56, 2013, pp. 11-26.

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net
Vol-20 Issue-01 April 2025

[5] Jin, X., He, W., & He, X. "AI-driven cyber risk prediction model for insurance premium calculation." Expert Systems with Applications, vol. 205, 2022, pp. 1-13.

[6] Wang, P., Wu, X., Liu, J., & Li, L. "Deep learning-based cyber threat intelligence for insurance risk assessment." IEEE Transactions on Information Forensics and Security,vol.17, 2022,pp. 1785-1799.

[7] Ganin,A.A.,Quach,P.,Panwar,M.,Collier,Z.A.,Keisler,J.M., Marchese, D., & Linkov, I. "Multicriteria decision framework for cyberriskinsurance."RiskAnalysis,vol.40,no.2,2020,pp.368-386.

[8] Baumgartner, S., Maillart, T., & Sornette, D. "Quantifying cyber risk and insurance premiums." The Geneva Risk and Insurance Review, vol. 44, no. 2, 2019, pp. 162-198.

[9] Eling,M.,&Wirfs,J.H."Cyberriskcharacteristicsandinsurance coverage."TheJournalofRiskandInsurance,vol.86,no.4,2019,pp. 823-851.

[10] Kesan,J.P.,Majuca,R.P.,&Yurcik,W."Cyberinsuranceasan incentivemechanismforcybersecurity."IllinoisPublicLawResearch Paper No. 08-05, 2008.

[11] Agrafiotis,I.,Nurse,J.R.C.,Goldsmith,M.,Creese,S.,&Upton, D."Ataxonomyofcyber-harms:Definingtheimpactsofcyber-attacks andunderstandinghowtheypropagate."JournalofCybersecurity,vol. 4, no. 1, 2018, pp. 1-15.

[12] Marotta,A.,Martinelli,F.,Nanni,S.,Orlando,A.,&Yautsiukhin, A. "Cyber-insurance survey." Computer Science Review, vol. 24, 2017, pp. 35-61.

[13] Pal, R., Golubchik, L., Psounis, K., & Hui, P. "Will cyber-insurance improve network security? A market analysis." IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 2014, pp. 235-243.

[14] Herath, H. S. B., & Herath, T. C. "Cyber risk analysis and mitigationusingBayesianinference."DecisionSupportSystems,vol. 86, 2016, pp. 56-66.

[15] Xu,L.,Chen,J.,&Whinston,A."Cybersecurityinsurance: Modeling and pricing." MIS Quarterly, vol. 35, no. 2, 2011, pp. 533-554.

[16] Böhme,R.,&Schwartz,G."Modelingcyber-insurance:Towards a unifying framework." Proceedings of the Workshop on the Economics of Information Security (WEIS), 2010.

[17] Shah, J., Saleh, M. N., & Kim, D. S. "AI-powered cyber risk assessment framework: Challenges and opportunities." IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, 2023, pp. 1021-1036.

[18] Gordon,L.A.,Loeb,M.P.,&Sohail,T."Aframeworkforusing insuranceforcyber-riskmanagement."CommunicationsoftheACM, vol. 46, no. 3, 2003, pp. 81-85.

[19] Radanliev,P.,DeRoure,D.,Nurse,J.R.C.,Nicolescu,R.,Huth, M.,&Montalvo,R.M."Cyberriskandsecurity:Asystematicanalysis of AI-driven cyber risk assessment models." Computers & Security, vol. 103, 2021, pp. 1-18.

[20] Johnson, B., Böhme, R., & Grossklags, J. "Security investment and cyber insurance: A game-theoretic analysis." Proceedings of the 2011 Workshop on the Economics of Information Security (WEIS), 2011.