IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE ASSESSMENT OF CYBER SECURITY'S SIGNIFICANCE IN THE FINACIAL SECTOR OF LITHUANIA

[1] Dr. T. LAKSHMI DEVI, [2] GANTHALA AKHILA, [3]ALETI VIVEK, [4] SUTHARI HARIKA, [5] ESURAJU MAHESH

[1]Associate professor, [2,3,4,5] UG STUDENT

[1,2,3,4,5]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(CSE)

[1,2,3,4,5]AVANTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

Gunthapally(V), Abdullapurmet(M), R.R Dist – 501512

ABSTRACT:

High-tech tools are changing fast, creating new ways to grow but also new risks that businesses don't know about. Cyber risk is one of the most significant risks in the financial sector of companies as online financial services and finance operations are part of everyday life. According to the survey conducted by the National Bank of Lithuania in late 2018, the possibility of cyber threats and their possible effects on the financial system of Lithuania is one of the most serious problems and should be given the highest priority. So, it's crucial to know which cyber threats in financial companies are the worst and most probable. Also, to know how companies in the financial sector rank their readiness and willingness to deal with this kind of cyber risk management and control. This research is important for financial institutions as a way to improve their cyber risk management processes, improve preparedness and cyber security and identify potential threats to the organization.

Keywords— Cybersecurity, Financial Sector, Risk Management, Machine Learning, Threat Detection, Data Protection,

1. INTRODUCTION

Information and communication technologies are in continuous progress, so the financial sector has been changed rapidly in the last few years. The modern way to do business is through online banking, digital payments, mobile financial services and cloud-based financial systems.[2] These new technologies have made things more efficient, more accessible, more convenient for customers. But they have also left financial institutions more exposed to different types of cyber threats. With financial services increasingly dependent on digital infrastructure, the implementation of strong cybersecurity measures has become a key priority for financial organisations globally.

Cybersecurity refers to protecting computer networks, systems and sensitive data from cyberattacks, intrusions and other digital threats. Cybersecurity is very important in the financial sector because banks and other financial institutions handle very private information such as customer data, transaction records, financial assets and private business information. If this information is leaked, it can cause huge financial

losses, damage your reputation, legal issues and loss of customer trust. Therefore, they must have good cybersecurity plans to ensure the stability and safety of financial systems.[3]

Like many other countries, Lithuania's digital financial ecosystem has grown rapidly. More people are using fintech services, online banking platforms and electronic payment systems, which has made the Lithuanian financial sector more integrated and high-tech.
However, this digital expansion has also increased the susceptibility of banks and other financial institutions to cyber threats such as phishing attacks, ransomware, data breaches, malware infections and distributed denial-of-service (DDoS) attacks. Cyber risk has emerged as one of the biggest threats to safety and stability of the financial system, the National Bank of Lithuania said.[4]
Basic security tools used by financial institutions to protect their systems include firewalls, antivirus software, and manual monitoring. These solutions provide a baseline level of protection, but they are often reactive and may not be able to find or stop more sophisticated cyber threats. Today cyberattacks are becoming more sophisticated, attacking system weaknesses, human errors and weak points in networks. That means banks and other financial institutions will need smarter, more proactive and more advanced cyber security solutions to deal with these new threats.[5]

So, it is important to see the importance of cybersecurity in the financial sector to know the extent of their preparedness, the major weaknesses and to find out how well they manage cyber risks. By examining potential cyber threats and existing safeguards, financial institutions can enhance their cybersecurity frameworks and bolster their defences. The paper presents a study of cyber risks in the Lithuanian financial sector and proposes an intelligent cyber risk management framework based on real-time monitoring, predictive analytics and automated threat detection.[6]

The proposed framework is expected to enhance cyber risk management through the use of advanced technologies such as AI, machine learning and centralised threat intelligence systems. [8]Such technologies enable banks and other financial institutions to detect threats earlier, react to them more rapidly and generally develop a greater employee awareness of security issues. At the end of the day, the enhancement of cybersecurity in the financial sector will contribute to securing financial assets, complying with regulations, maintaining the trust of consumers and ensuring the long-term stability of the financial system.[7]

3.LITERATURE SURVEY:

Recent research shows that cybersecurity is becoming more and more important in the financial industry as digital technologies are being increasingly adopted. Kshetri (2016) research indicates that financial institutions are targets of cyber criminals because their digital assets and financial data are of high value. Phishing, ransomware, malware, insider attacks – these are just a handful of the many threats that can impact financial operations and expose sensitive data.[9]
The Basel Committee on Banking Supervision (2018) says that we need full cyber security frameworks including risk assessment, monitoring and incident response. [10]Their research shows that proactive cybersecurity can reduce financial losses and make operations more resilient. Similarly, AI studies in cybersecurity show that machine learning algorithms can analyse a huge amount of data simultaneously to detect abnormal patterns and predict cyber threats in real-time. This is better than rule-based system[11]
Research on cyber threat intelligence has demonstrated that the use of data from multiple sources, including security logs and external threat feeds, can enhance situational awareness and decision making.[12] Further improvement in security can be achieved with real-time monitoring systems to detect anomalous activities and reduce the response time to cyber incidents. Research in human factors also reveals that employee awareness and training are very important in preventing security breaches as human error is a major cause of cyber incidents.[13]
Overall, the literature supports the use of advanced technologies, real-time monitoring and awareness programs in organisations to improve cybersecurity in banks and other financial institutions.[14]. Nevertheless, the need for a unified and intelligent system that efficiently integrates these components remains, which is addressed by the proposed system.[15]

4. METHODOLOGY:

The proposed system provides a systematic approach to develop an Intelligent Cyber Risk Management and Control Framework for banks and other financial institutions. The first step is to collect data from a variety of sources, including network logs, transaction records and user behaviour within the system. We look at this information for possible weaknesses and cyber risks that could threaten the financial system.
Cutting-edge technologies like machine learning and predictive analytics are then used to find patterns and pinpoint problems as they happen. The system uses AI-based models to classify threats, assess their risks and attempt to predict cyberattacks before they occur. This proactive approach helps businesses to avoid problems before they happen, rather than after they happen.
The system comprises several modules, including threat intelligence, risk assessment, real-time monitoring, incident detection, and employee awareness. Together, these modules provide continuous monitoring, automatic threat detection and rapid response. The framework also includes reporting and visualisation tools to help decision-makers understand cybersecurity risks and do the right thing.
This approach generally emphasises the incorporation of intelligent technologies, real-time surveillance, and anticipatory risk mitigation techniques to enhance cybersecurity in the financial industry.

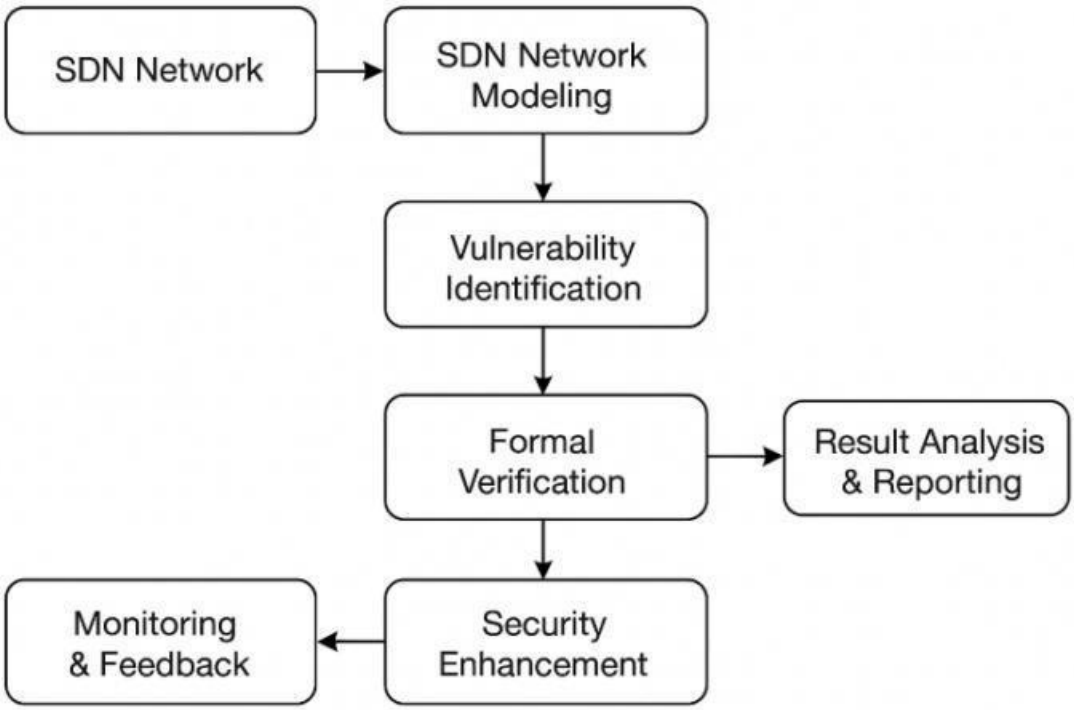
4.1 DATASET:

The dataset used in this system consists of cybersecurity related data from financial institutions such as network traffic logs, user behaviour data, transaction data and historical cyberattack data. The dataset is intended to allow for the development of machine learning models for threat detection and risk analysis. This contains labelled data of different types of cyber threats, such as phishing, malware, and unauthorised access attempts. This dataset allows the system to learn patterns, detect anomalies, and improve the accuracy of threat detection over time.

4.2. ALGORITHM :

Algorithm: AI-Driven Cyber Threat Detection
D. Network Data
Output: THREAT WARNING (T)
Steps:
1. Start 2.
2. Obtain network and transaction data
3. Data Preprocessing (Cleaning, Normalisation)
4. Feature extraction from the data
5. Application of the model
6. Anomaly detection and threat classification
7. Generation of threat alerts
8. Save the results for future learning
9. Project end

4.3. SYSTEM ARCHITECTURE:



5.RESULT ANALYSIS:

The findings reveal that the proposed intelligent cybersecurity framework can greatly improve the detection and management of cyber threats in financial institutions. The system continuously monitors the network activities in real-time and identifies the suspicious patterns with the help of machine learning algorithms. This allows early detection of cyber threats thereby reducing the probability of financial losses and system breakdowns.

A centralised dashboard can be deployed to visualise the cybersecurity metrics, monitor alerts and analyse the threat patterns efficiently by the administrators. Automated incident response mechanisms enhance system performance by reducing response time and mitigating the impact of cyber attacks. Moreover, staff training modules increase awareness and reduce vulnerabilities associated with human factors.

In conclusion, the system is more efficient, accurate and reliable than the traditional cyber security systems, therefore it is a valuable solution for the modern financial systems.

6 . CONCLUSION :

As digital technologies increasingly drive the financial services sector, cybersecurity is a crucial element in maintaining system stability and safeguarding sensitive information. The article points out the importance of cybersecurity in the Lithuanian financial sector and discloses the main challenges of traditional security systems. The results indicate that reactive security measures are not sufficient to deal with the ever-growing complexity and sophistication of cyber threats today.

The proposed Intelligent Cyber Risk Management and Control Framework is a holistic framework integrating AI, machine learning, predictive analytics and real time monitoring. This methodology enables better risk management, quicker response and easier threat identification before they occur. It is easier to make an organisation safer when you add employee awareness programmes that address the vulnerabilities that come from people.

The system is a scalable, efficient and smart way to improve the cybersecurity of financial institutions. Possible further improvements are the implementation of state-of-the-art deep learning algorithms, blockchain and cloud security systems for the enhancement of the cybersecurity architecture and for its protection against new cyberattacks over time.

REFERENCES

[1]. Dr. N. Satyavathi, Dr. Eppakayala Balakrishna, "Mining of Association Rules from Big Data Sets", Journal of Technology, PageNo:-1018-1024, volume 13, Issue 6, 2025, DOI: 18.15001/JOT.2025/V13I6.25.1672 (SCOPUS)
Link: https://journaloftechnology.org/volume-13-issue-6-2025

[2]. Dr.N. Satyavathi, K. Karthik, G. S. Vamshi and B. Shivasai, "Predictive modelling approach for sleep disorder using sleep health and lifestyle properties," Journal of Computational Analysis and Applications (JoCAAA), vol. 34, no. 4, pp. 482–492, 2025. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6463351/
Link : https://eudoxuspress.com/index.php/pub/article/view/2329 [3]. Dr.N. Satyavathi, A. Sharanya, S. Vishesh, and S. Modam, "Blockchain powered police complaint management system," International Journal of Communication Networks and Information Security (IJCNIS), vol. 17, no. 3, pp. 656–665, 2025, doi: 10.48047/IJCNIS.17.3.656-665. [Online]. Available: https://www.ijcnis.org/index.php/ijcnis/article/view/8204 [4] Dr.N. Satyavathi, G. S. Rani, P. Shashikanth, N. Afiya, and K. Pranay, "AI-powered Django framework for multi-class classification of skin disease for enhanced diagnosis," Journal of Computational Analysis and Applications (JoCAAA), vol. 34, no. 4, pp. 392–404, 2025.
Link: https://www.eudoxuspress.com/index.php/pub/article/view/2312 [5]. Dr.N. Satyavathi, Dr.E. Balakrishna, "IoT based solar powered agriculture," International Journal of Innovative Management and Scientific Research (IJIMSR), vol. 2, no. 2, pp. 18–24, 2024.
[6] Dr.N. Satyavathi,Dr. E. Balakrishna, and G. Shravya, "IoT-based smart irrigation system integrated with machine learning for crop yield prediction", Industrial Engineering Journal, vol. 53, no. 10, Oct. 2024, ISSN: 0970-2555. Link: https://ijimsr.org/abstract.php?id=35
http://www.journal-iiie-india.com/1_oct_24.html
http://www.journal-iiie-india.com/1_oct_24/1_online_oct.pdf

[7]. Dr.N. Satyavathi, K. Laya, S. Kumar B., and Dr.E. Balakrishna, "CO2 emission rating by vehicle using data science," Industrial Engineering Journal, vol. 53, no. 9, Sep. 2024, ISSN: 0970-2555.
Link: http://www.journal-iiie-india.com/1_sep_24.html [8]. B. Sindhu, T. Jahan, Dr.E. Balakrishna, and Dr.N. Satyavathi, "Image processing techniques for counterfeit currency detection", Journal of Engineering Sciences, vol. 15, no. 11, 2024. (SCOPUS).
Link: http://www.jespublication.com/issue.php?cid=26&scid=113

[9]. M. Anupama, Dr.N. Satyavathi, Dr.E. Balakrishna, "A knowledge-based recommendation system with sentiment analysis and deep learning", International Journal of Progressive Research in Engineering Management and Science (IJPREMS), vol. 4, no. 8, pp. 156-164, Aug. 2024, e-ISSN: 2583-1062.
https://www.ijprems.com/paperdetail.php?paperId=bb557951ed7ed8c535b897bcc1d9ee98&title=A+Knowledge+Based+Recommendation+System+Incorporating+Sentiment+Analysis+and+Deep+Learning&authpr=Mateti+Anupama

[10]. Dr.N. Satyavathi, K. Tharun, G. Pranay, K. D. Chand and P. S. Prakash, "Detection of autism spectrum disorder using machine learning," Industrial Engineering Journal, vol. 53, no. 5, May 2024.
The following link can be used to access the article: http://www.journal-iiie-india.com/1_may_24/6_online_may.pdf
Link: http://www.journal-iiie-india.com/1_may_24.html [11]. Dr.N. Satyavathi, Y. Vineeth, R. Sreya, D. MalvikanRaj, and K. Vaibhav, "Proficient allocation of resources and time arrangement", JuniKhyat (जूनीख्यात), vol. 14, no. 5, May 2024, ISSN: 2278-4632.
www.junikhyatjournal.in/no_1_Online_24/23_online_may.pdf
http://junikhyatjournal.in/no_1_Online_24.html

[12] N. Satyavathi, V. Poojitha, E. Sushma, D. Vinitha, and C. B. Monica, "Attribute identification of campus based college attendee using data mining," Journal of Nonlinear Analysis and Optimisation, vol. 15, no. 1, 2024.

The link is https://jnao-nu.com/Vol.%2015,%20Issue.%2001,%20January-June%20:%202024/147.15.pdf

[13]. Dr.N. Satyavathi, G. Vennela, A. Rishika, G. Manohar, and A. Sanjana, "A Unique travel plans with a cocktail touch approach," Industrial Engineering Journal, vol. 53, no. 5, May 2024.
Link : http://www.journal-iiie-india.com/1_may_24/15_online_may.pdf [14]. N. Satyavathi and E. Balakrishna, "Market basket analysis using minimum lift-to-confidence ratio technique in data mining," Industrial Engineering Journal, vol. 52, no. 9, pp. 2–10, Sep. 2023.
Link : http://www.journal-iiie-india.com/1_sep_23/2.2_sep.pdf Link : http://www.journal-iiie-india.com/1_sep_23.html [15]. N. Satyavathi and E. Balakrishna, "Understanding security requirements, issues and challenges in Internet of Everything," International Journal of Computer Science Trends and Technology (IJCST), vol. 11, issue 4, Jul.–Aug. 2023.
https://www.ijcstjournal.org/volume-11/issue-4/IJCST-V11I4P10.pdf
https://www.ijcstjournal.org/Vol11Issue4No1.html

[16]. Dr.N. Satyavathi, Dr.E. Balakrishna, "Forecasting student achievement: Exploring data mining techniques in education", International Journal of Research in Academic World (IJRAW), vol. 1, no. 16, Dec. 2022.
Link: https://academicjournal.ijraw.com/media/post/IJRAW-1-16-57.1.pdf
https://academicjournal.ijraw.com/archive/y2022/v1/i16/December?page=5

[17]. Dr. E. Balakrishna, Dr.N. Satyavathi, "Seamless integration of edge computing and cloud resources for enhanced data analysis", International Journal of Scientific Research and Engineering Management (IJSREM), vol. 6, no. 11, Nov. 2022.
Link: https://ijsrem.com/download/seamless-integration-of-edge-computing-and-cloud-resources-for-enhanced-data-analysis/

[18]. G. Saikumar and Dr.N. Satyavathi, "Stock market analysis with various machine learning and deep learning algorithms," Journal of North Eastern University, vol. 26, no. 2, 2023. (SCOPUS).
Link: https://xuebao.neu.edu.cn/natural/EN/article/showOldVolumn.do

[19] . N. Satyavathi and B. Rama, "Present state of the art of dynamic association rule mining algorithms," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 9, no. 1, Nov. 2019. ISSN: 2278-3075. (SCOPUS).
Link: https://www.researchgate.net/publication/364095160_Present_State-of-The-ART_of_Dynamic_Association_Rule_Mining_Algorithms
https://www.ijitee.org/portfolio-item/a4107119119/ [20] Satyavathi, N. & B, Rama & Autha, Nagaraju. (2019). Present State-of-Art of Association Rule Mining Algorithms", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, (Online), Volume-9, Issue-1, October, 2019 (SCOPUS).
A2202109119