e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 6, Issue 6, June 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

Global Fortification - Unifying Global DDoS Defense

Govindarajan Lakshmikanthan, Sreejith Sreekandan Nair

Independent Researcher, Leading Financial Firm, Texas, USA

Independent Researcher, Leading Financial Firm, Texas, USA

ABSTRACT: Financial sector is enduring the painful effects of millions of dollars spent each month to combat dangerous DDoS attacks on bank services. Sometimes these attackers cloud the websites of banks to such an extent that critical services have to be halted, resulting in huge losses and reputational damage to the Company (Aljuhani, 2021). In this work, we demonstrate an artificial intelligence-based approach that detects and counteracts DDoS attacks aimed specifically at bank websites. Ensuring a high level of service for DDoS – attacked websites, this system helps to reduce financial loss due to service downtimes and as well as excessive transaction outages for clients. Furthermore, this model restricts aggressors, and implements a level of interbank information exchange regarding actual attacks. This research proposes a system for DDoS attack prevention that minimizes economic damage through the use of machine learning, which can improve the overall performance of any financial institution cybersecurity efforts. Additionally, this system integrates real – time navigation with historical data of DDoS attacks, which gives 'forward looking' capabilities in threat detection. It is important to note that a sophisticated anomaly detection system enables the proposed solution to significantly outperform standard models by disabling meaningful traffic while launching attacks from spurious IP addresses. This study also confirms deliberative modelled trials aimed at showing that the system is capable of greatly reducing the severity of DDoS attacks. In addition, the implemented solution provides a feasible and easily extensible approach that can easily be incorporated in the current bank's infrastructure. The research also speaks of the possibility of crowd-sourced threat intelligence, where banks would share anonymized data related to attacks for better security.

KEYWORDS: DDoS, Cyber Security, IAM, STIX, TAXII

I. INTRODUCTION

Today, every business activity is of critical importance. The need for sufficient protection against Denial of Service type attacks, which can render online systems inoperable and result in enormous financial harm, is greatly amplified. With traditional IAM systems meeting their limitations, a shift towards AI based models, which operate as shields as the first level of defense. Utilizing extensive network datasets, self-learning algorithms are able to identify inconsistencies that potentially are red flags for attacks. With preemptive measures such as adapting the infrastructure and rerouting traffic, a large majority of the attack get invalidated. Further development in Artificial Intelligence, and other computing technologies advances these systems past the current level of passive security providing a responsive, active threat management which in many cases will be able to predict and incapacitate an assault before it reaches a system. The response and intelligence of the system is based on Advanced neural networks, trained on global threat intelligence. The results show that protocols can be modified in real time and the time taken to respond to threats can be reduced from minutes to milliseconds. Faster response times mean less downtime, mitigated chances of data incidents and millions saved while instilling trust in digital businesses that can protect their customers intelligently. Artificial intelligence is set to transform future approaches to cybersecurity by demonstrating its application to augment cyber threats which is arguably the blueprint of a more sophisticated cyberspace marketplace.

II. RELATED WORK

Various approaches have been explored to combat DDoS attacks, including detection mechanisms and mitigation strategies. However, the evolving nature of these attacks, along with the increasing complexity of modern network architectures, has rendered many existing solutions incomplete or ineffective. While some techniques focus on making the attack more difficult or holding the attacker accountable, a comprehensive and unified defense mechanism remains elusive. Researchers have explored the use of deep learning and Gaussian Mixture Models to detect unknown DDoS attacks (Shieh et al., 2021), and have proposed hybrid deep learning models with improved feature selection to efficiently detect DDoS attacks (Alghazzawi et al., 2021). However, these approaches still face limitations in dealing with the open set recognition problem, where the machine learning-based systems fail to properly identify new instances that do not conform to the training data distribution. (Shieh et al., 2021). As revealed in the research,

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

Recurrent Neural Networks can be incorporated to identify these attacks, as human brain is more perfect than mathematical computation" (Islam & Sabrina, 2009). According to (Shieh et al., 2021), the detection of DDoS attacks is a challenging issue before any mitigation measures can be taken. Researchers have explored the use of machine learning-based approaches to detect DDoS attacks, with a focus on improving the efficiency, operating load, and scalability of these systems. (Atasever et al., 2020) However, a key limitation of these approaches is the "open set recognition problem," where the machine learning models fail to properly identify new instances that do not conform to the training data distribution. To address this limitation, researchers have proposed the use of deep learning and Gaussian Mixture Models to detect unknown DDoS attacks. This approach has shown promising results, but further advancements are still needed to fully address the complexities of modern DDoS attacks. Furthermore, a hybrid deep learning model with improved feature selection has been developed to efficiently detect DDoS attacks. This model combines the strengths of various deep learning techniques, along with an enhanced feature selection process, to achieve improved accuracy and performance in DDoS attack detection. In addition to these technical advancements, the research also highlights the importance of incorporating human intelligence and intuition in the detection of DDoS attacks.

III. PROPOSED ALGORITHM

Traditional methods of authentication and authorization are proving to be inadequate in the face of sophisticated cyber threats in today's rapidly evolving digital environment. This phase presents a shift from a static, rule-based password and authorization to a flexible AI-driven authentication authorization system. This new system leverages the power of

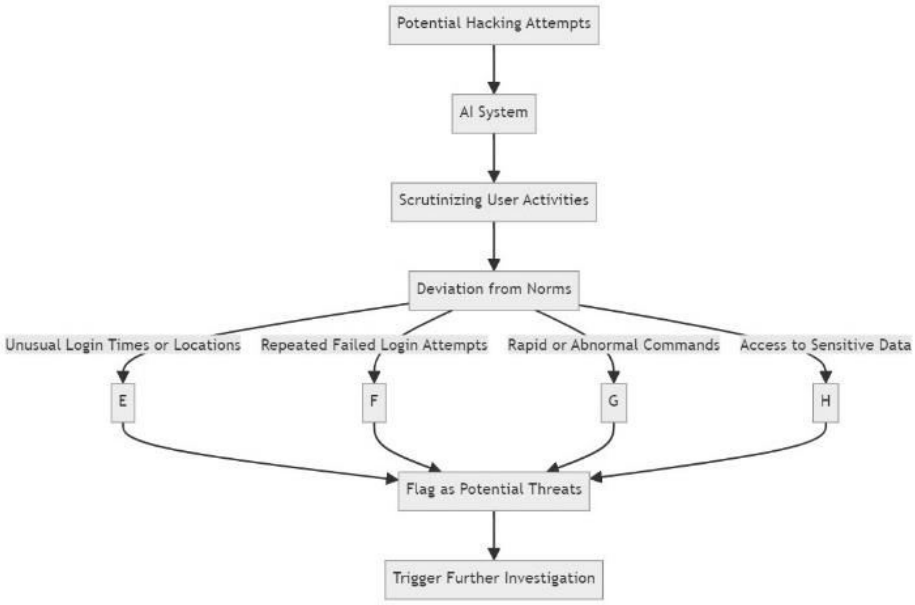

Figure 1: Detecting Anomalous Behavior

artificial intelligence to analyze user behavior in real time and distinguishes between a legitimate login and a malicious attempt with unprecedented accuracy and efficiency. At the core of this sophisticated fortem are advanced machine learning algorithms, akin to digital spies, that scrutinize every user action and discover complex patterns in data unlike traditional approach leverages authentication based solely on personal identifiers, such as username and password. It captures and analyzes countless pieces of non-personal data from every user interaction, from keystroke dynamics to mouse movements down to device attributes and even location data. Every aspect of user behavior contributes to the creation of unique behavioral fingerprints. At the core of this behavioral analysis engine are advanced machine learning models that can effectively capture complex user behavior patterns. Unsupervised learning techniques like clustering algorithms (k-means, DBSCAN) group user behaviors into normal and anomalous clusters without requiring labeled data. Dimensionality reduction methods (PCA, t-SNE) identify the most important behavioral features from high-dimensional data. Outlier detection models (Isolation Forests, One-Class SVMs) specifically flag anomalous user activities deviating from normal patterns. Sequence learning models like Recurrent Neural Networks (LSTMs, GRUs) excel at modeling sequential user events and capturing long-term dependencies. Markov models represent user behavior as transitions

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

between different states based on probabilities learned from data. Ensemble methods combining multiple models, such as Random Forests and Gradient Boosting machines (XGBoost, LightGBM), can further boost predictive performance through majority voting or sequential error correction. Consider a typical login scenario: Instead of being greeted with a static username/password prompt, users are easily authenticated via a one-step fingerprint scan This frictionless authentication process can trigger a multifactor verification challenge, ensuring an additional layer of security, if require.

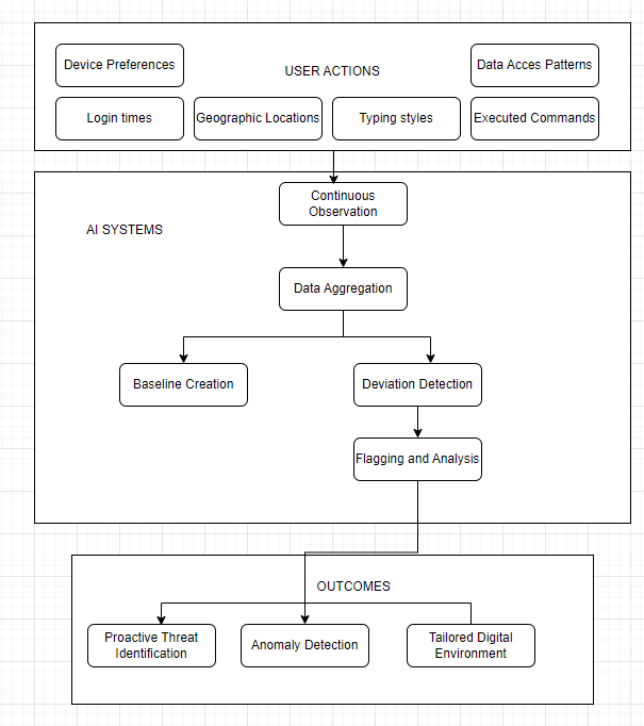

Figure 2: DDos Component Diagram

Flexible nature of the system allows the authentication level to be dynamically adjusted in real time, and it effectively prevents potential threats and reduces the risk of unauthorized access. The real power of an AI-driven system lies in its ability to detect suspicious activity and respond with unparalleled speed and accuracy. Emergency password failures or login attempts from an unknown location are not recognized as isolated incidents but are flagged as potential security risks. When analyzed by AI system, it triggers immediate action to mitigate the threat, or additional steps to validate it, all in real time, without compromising the user experience. In addition to the role of security improvements, AI-driven authentication and authorization offers many benefits that extend to both users and organizations. By personalizing authentication levels based on individual behavior patterns, the system reduces burdensome authentication barriers for legitimate users, resulting in a seamless and frictionless experience. It eliminates associated inherent weaknesses, ensuring that security measures evolve in line with emerging threats. From an economic perspective, the adoption of AI-powered security solutions means significant cost savings for organizations. By streamlining security measures and minimizing security breaches, organizations can reduce the financial and reputational costs associated with cyberattacks and further contribute to overall system more cost-effective by reducing the effort in customer service for password resets and queries. Looking ahead, the implications of AI-powered security systems are profound.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

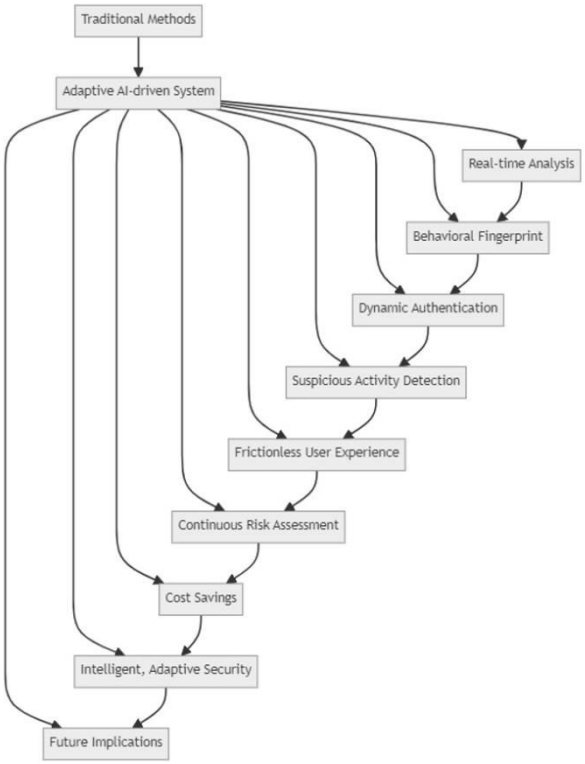

Figure 3: Transformation to AI-driven security

As digital adversaries become more sophisticated, the need for intelligent and adaptive security measures is more important than ever. As advances in AI technology continue to push the boundaries of what's possible, the future of digital security holds great promise. An AI-powered authentication authorization system isn't just a passive watchdog - it's a proactive watchdog, learning from every interaction and evolving to stay one step ahead of potential threats.

IV. INFORMATION SHARING AMONG FINANCIAL INSTITUTIONS

The Threat Information Sharing Mechanism is the cornerstone of the proposed counter-threat intelligence system, serving as the vital conduit through which participating institutions exchange real-time threat intelligence. This mechanism enables institutions to contribute and access crucial details of detected threats, empowering them to fortify their cyber defenses and mount a unified response against malicious actors. Let's delve deeper into the key components and implementation strategies of this mechanism:

IP Addresses:
IP addresses serve as crucial identifiers of the network origin of malicious activity. By sharing information on suspicious or known malicious IP addresses, institutions can collectively identify and block malicious traffic, preventing unauthorized access and potential data breaches. The inclusion of IP addresses in the threat intelligence repository enables institutions to stay vigilant against evolving cyber threats and proactively safeguard their networks.

Device Fingerprints:
Device fingerprints play a pivotal role in tracking devices used repeatedly in attacks. By sharing information on device fingerprints associated with malicious activities, institutions can identify compromised or hijacked devices used by cybercriminals to orchestrate attacks. This enables institutions to detect and mitigate threats at an early stage, preventing further exploitation of compromised devices and minimizing the risk of widespread damage.

Malware Signatures:
Malware signatures are characteristic patterns that signal the presence of specific malware strains or variants. By sharing information on malware signatures, institutions can collectively identify and block known malware threats, thwarting their proliferation across networked environments. This proactive approach to malware detection and

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

prevention helps in containing the spread of infections and mitigating the impact of malware-driven attacks on critical systems and data.

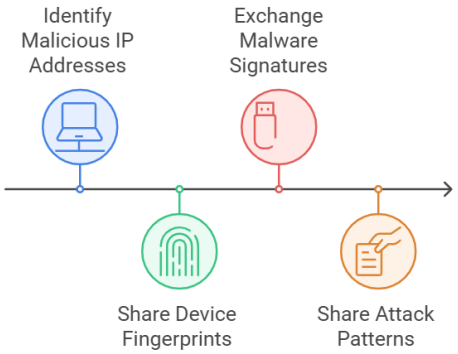

Figure 4: Threat Information Sharing mechanism

Attack Patterns:
Attack patterns refer to recognizable sequences of actions executed by attackers during cyber-attacks. By sharing information on attack patterns observed in real-time, institutions can gain insights into the tactics, techniques, and procedures (TTPs) employed by threat actors. This enables institutions to anticipate and defend against emerging cyber threats more effectively, thereby enhancing their overall cyber resilience and readiness to combat sophisticated attacks.

Distributed Ledger:
The sharing mechanism can be implemented using either a centralized database or a distributed ledger, such as blockchain, depending on the specific requirements and priorities of participating institutions. A centralized database offers simplicity and ease of access, allowing institutions to quickly share and retrieve threat intelligence data. However, concerns about data security, integrity, and single points of failure may arise with this approach. On the other hand, a distributed ledger, like blockchain, offers enhanced security and immutability by decentralizing the storage and verification of threat intelligence data across a network of nodes. Each participating institution maintains a copy of the blockchain, ensuring transparency, trust, and resilience against tampering or unauthorized modifications. Additionally, the use of cryptographic techniques, consensus mechanisms, and smart contracts can further bolster the security and integrity of the shared threat intelligence data on the blockchain. By pooling together, the intelligence and resources of the financial community, the collaborative approach creates a formidable barrier against cyber threats. When one participant detects a threat, they can quickly share this information with others, enabling swift action to neutralize the threat across multiple institutions. This collective response significantly improves overall protection by leveraging the combined expertise and insights of multiple stakeholders. Instead of each institution facing threats in isolation, they benefit from a shared defense mechanism that enhances their ability to detect, respond to, and mitigate cyber risks effectively. In a collaborative environment, threats are identified and neutralized with unprecedented speed. Real-time threat information sharing enables participating institutions to stay ahead of emerging cyber threats and take proactive measures to defend their networks. As soon as a threat is detected by one participant, others can be alerted, enabling a coordinated response to neutralize the threat before it can inflict significant damage. This rapid response capability minimizes potential downtime, data loss, and financial impact, thereby mitigating the consequences of a breach and preserving the integrity of critical systems and data.

Sharing threat data among participating institutions leads to significant cost savings. Instead of each institution investing in developing and managing independent threat intelligence programs, they can collectively contribute to and benefit from a single shared system. This shared approach reduces duplication of efforts, eliminates the need for redundant infrastructure, and lowers operational costs associated with maintaining separate threat intelligence capabilities. By leveraging economies of scale, participating institutions can achieve greater efficiency and effectiveness in their cybersecurity efforts while optimizing resource allocation and maximizing return on investment.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

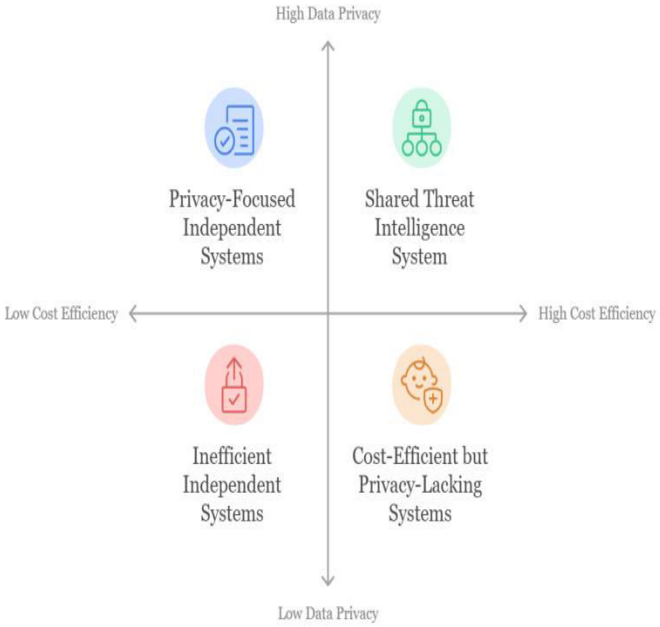

Figure 5 : Balancing Cost Efficiency and Data Privacy

Protecting the privacy of customers and organizations sensitive data is paramount. The system must incorporate robust mechanisms to safeguard sensitive information from unauthorized access, disclosure, or misuse. This can be achieved through the implementation of anonymity procedures, encryption protocols, and strict access controls. Additionally, clear data retention policies should be established to govern the data collection, data storage, and data disposal of shared data in compliance with applicable privacy regulations, such as GDPR or CCPA. By prioritizing data privacy, the system can foster trust among participants and ensure the ethical handling of sensitive information. Shared data should adhere to well-defined standards and protocols to ensure consistency, interoperability, and seamless integration across different systems. Establishing common data formats, schemas, and metadata standards enables participating institutions to exchange information effectively and derive actionable insights from shared intelligence. By adopting industry-recognized standards, such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information), the system can facilitate the efficient exchange of threat intelligence while minimizing compatibility issues and data inconsistencies.

Continuous Learning and Adaptation

The key advantage of using AI for behavioral analysis is its capability to learn and adjust to changing circumstances. Unlike rule-based systems, which are created and designed to be unresponsive to change, AI-based systems have the advantage of undergoing improvement and evolution through learning as well adjusting to new situations. One area that is important during this learning process is how the system establishes new normal which is to be the baseline of behavior for both users and, in some cases, their systems. When users perform some actions on a digital environ and its respective systems, the AI system watching them tries to create a framework of such actions and their relevance to other performed non-target actions. This framework is not constant; later on, it increases with the amount of gathered information about the actions taken by the user and how he would carry them out in the future. Additionally, such a system regularly updates its algorithms for detecting anomalies in automated systems and manual users' actions with the ultimate goal of determining what behavior is abnormal. The system includes a feedback mechanism whereby previous actions taken to protect the baseline set of activities feed into improving the analysis of new variations from that baseline.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

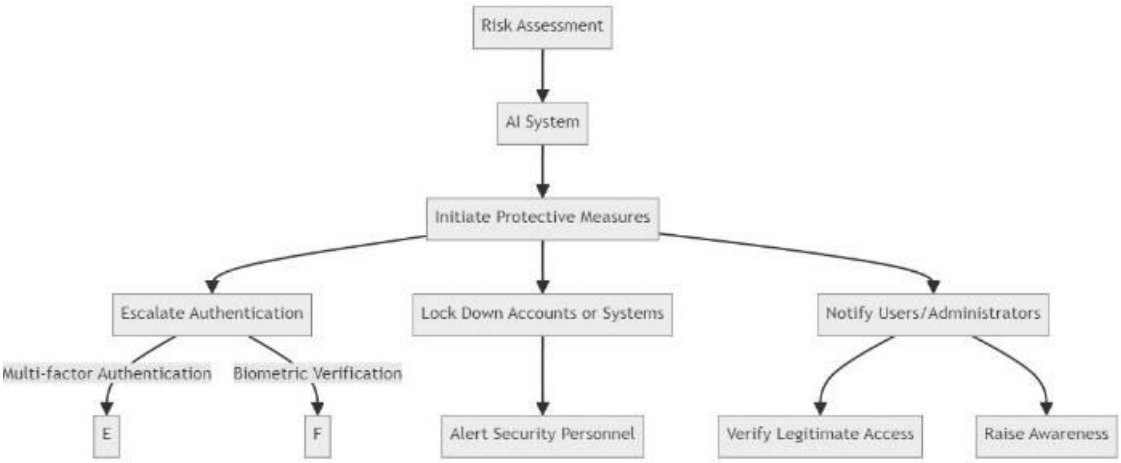

Figure 6: Proactive Measures

This optimization procedure allows the system to become more sensitive and precise in action against real threats and drastically cut down on false alarms. Besides enhancing the algorithms for anomaly detection, the AI system updates its models for risk assessment according to the changing threat scenarios and firm's strategies. Such integration allows the system to assess the risks in a more effective way regarding the extent and the damage that an anomaly might cause to the organization. Such a method of usage allows one to ensure that the system's risk assessment will be applicable against new unforeseen cyber security hazards. It is this cyclic process of learning and adaptation that makes the AI based behavioral analytics system more effective as it gets older and older as well as asymmetrically staying above the threat curve. The AI system consistently aggrandizes its baseline of normalcy or behavior, coping with parameters of anomaly anti-detection algorithms, making changes to models of risk assessment, and integrating new threat intelligence all strengthen the systems' capability to detect and manage automatically security risks in real accordingly. In order to constantly learn from data streams of new interactions of users with the system, the system utilizes online learning algorithms such as Vowpal Wabbit (VW). The design of VW allows for the sequential processing of data instances, which permits the system to incrementally refine its predictive models as further data is accumulated over time. This ability is paramount so as to assure that the system's behavioral models and risk assessment capabilities are adapted to the status quo in terms of new threats and novelty.

V. SIMULATION RESULTS

The AI-driven authentication and authorization system marks a paradigm shift in digital security. It represents the culmination of years of research and innovation, offering a glimpse into the future of security - intelligent, adaptive, and always vigilant. As organizations navigate the ever-changing threat landscape, embracing these innovative technologies is paramount. By harnessing the power of artificial intelligence, organizations can enhance their security posture, safeguard sensitive data, and ensure a seamless user experience in an increasingly digital world.

Establishing Normal Behavioral Patterns

In the realm of digital security and optimization, AI systems play a pivotal role in continuously observing user behavior. This includes monitoring a spectrum of parameters like login times, geographic locations, device preferences, typing styles, executed commands Through data aggregation, the AI system creates personalized baselines for each user or group, reflecting their typical behaviors. These baselines act as benchmarks against the threshold deviation. When deviations occur, the system flags and analyzes it, discerning between benign changes and potential security threats or anomalies. This process enables proactive identification and response to suspicious activities, ensuring a safer and more efficient digital environment tailored to individual or group behaviors.

VI. CONCLUSION AND FUTURE WORK

The proposed collaborative system offers a transformative strategy to elevate cybersecurity resilience within the intricate ecosystem of the financial industry. Its core premise lies in the collective sharing of threat intelligence among banks and institutions, fostering a dynamic network where information is leveraged to anticipate and counter cyber

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

threats swiftly and effectively. This collaborative framework enables participants to transcend the limitations of isolated defense mechanisms, creating a unified front against the ever-evolving landscape of cyber threats. By embracing a culture of information sharing, banks and financial institutions can tap into a vast repository of collective knowledge and experiences. Through real-time sharing of threat information, organizations gain invaluable insights into emerging attack vectors, malicious trends, and evolving tactics employed by cyber adversaries. This heightened awareness not only enhances the ability to detect and thwart imminent threats but also empowers institutions to proactively fortify their defenses against future attacks. The essence of collaboration lies in the ability to learn from each other's successes and failures. By analyzing shared threat data and incident reports, institutions can extract valuable lessons and best practices, refining their cybersecurity strategies and bolstering their resilience against similar threats. Furthermore, the collaborative exchange of threat intelligence facilitates a rapid response mechanism, enabling institutions to mobilize resources and coordinate efforts to mitigate the impact of cyber incidents in real-time. This agility in response is paramount in minimizing disruption, containing damages, and safeguarding critical assets and customer information. However, the success of this collaborative endeavor hinges on addressing several critical challenges. Foremost among is the imperative to safeguard data privacy and confidentiality. Striking the delicate balance between sharing threat information and protecting sensitive customer and organizational data necessitates robust mechanisms for anonymization, encryption, and access control. Furthermore, the establishment of clear standards and protocols is essential to ensure the consistency, accuracy, and interoperability of shared threat intelligence data across diverse systems and platforms.

Adherence to industry-recognized standards such as STIX and TAXII facilitates seamless integration and maximizes the utility of shared threat intelligence resources. Adequate governance mechanisms must be put in place to oversee the management and functioning of the collaborative system. Clear policies and procedures are needed to define participation requirements, delineate roles and responsibilities, and establish mechanisms for resolving disputes and enforcing compliance. By fostering transparency, accountability, and trust among participants, robust governance mechanisms provide confidence, integrity and reliability of the collaborative platform. Ultimately, if these challenges are met with diligence and foresight, the collaborative approach holds immense potential to revolutionize cybersecurity readiness across the entire financial sector. By harnessing collective intelligence, expertise, and community resources, institutions can forge a resilient defense posture capable of withstanding the most sophisticated cyber threats. In an era marked by relentless cyber-attacks and escalating risks, the collaborative system stands as a beacon of hope, offering a path towards a safer, secure digital future for the financial industry and its stakeholders.

REFERENCES

[1] A. Aljuhani, “Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments,” Jan. 01, 2021, Institute of Electrical and Electronics Engineers. doi: 10.1109/access.2021.3062909.
[2] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
[3] Debar, H., Curry, D., & Feinstein, B. (2007). The intrusion detection message exchange format (IDMEF) (No. RFC 4765).
[4] Husák, M., Čermák, M., Laštovička, M., & Vykopal, J. (2020). Employee behavior and computational behavior models for insider threat detection. Frontiers in Computer Science, 2, 22
[5] Roy, S. S., Pallampati, R., Saideep, C., & Augustine, J. (2021). A vision of collaborative intelligence for cyber defense. IEEE Systems Journal, 16(2), 2457-2469
[6] Sillaber, C., Hutter, R., Gindl, S., & Mahr, B. (2016). Behavioral patterns and insider threat detection. In ARES 2016: 11th International Conference on Availability, Reliability and Security (pp. 638-643).
[7] STIX, T. (2018). Structured threat information expression (stix) version 2.1. OASIS Committee Specification Draft 01. Retrieved from https://oasis-open.github.io/cti-documentation/stix/intro
[8] D. Alghazzawi, O. Bamasag, H. Ullah and M. Z. Asghar, "Efficient Detection of DDoS Attacks Using a Hybrid Deep Learning Model with Improved Feature Selection," Appl. Sci., vol. 11, no. 24, p. 11634, 2021, doi: 10.3390/app112411634.
[9] Thai Son Chu, Sreejith Sreekandan Nair, Govindarajan Lakshmikanthan 2022. Network Intrusion Detection Using Advanced AI Models A Comparative Study of Machine Learning and Deep Learning Approaches. International Journal of Communication Networks and Information Security (IJCNIS). 14, 2 (Aug. 2022), 359–365.
[10] S. Atasever, İ. Özçelik and Ş. Sağıroğlu, "An Overview of Machine Learning Based Approaches in DDoS Detection," in Proc. 30th Signal Process. Commun. Appl. Conf. (SIU), 2020, doi: 10.1109/siu49456.2020.9302121.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 6, Issue 6, June 2023 |

| DOI:10.15680/IJMRSET.2023.0606054 |

[11] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Comput. Netw., vol. 44, no. 5, pp. 643-666, 2003, doi: 10.1016/j.comnet.2003.10.003.
[12] A. B. M. A. A. Islam and T. Sabrina, "Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble," vol. 38, p. 603, 2009, doi: 10.1109/iccit.2009.5407308.
[13] C. Shieh et al., "Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model," Appl. Sci., vol. 11, no. 11, p. 5213, 2021, doi: 10.3390/app11115213.
[14] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2046-2069, 2013, doi: 10.1109/surv.2013.031413.00127.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com