International Research Journal of Innovations in Engineering and Technology(IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 299-306, November-2023
https://doi.org/10.47001/IRJIET/2023.711041

Security Operation Center for Healthcare Sector

[1]Abeysinghe A.M.S.B., [2]De Zoysa M.T.R., [3]Samuditha K.M.Y., [4]Dissanayake D.J.D.H.T., [5]Kanishka Yapa [6]Uditha Dharmkeerthi

[1,2,3,4,5,6]Faculty of Computing, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka
Authors E-mail: [1]it20146542@my.sliit.lk, [2]it20200138@my.sliit.lk, [3]it20204266@my.sliit.lk, [4]it20255138@my.sliit.lk, [5]kanishka.y@sliit.lk, [6]uditha.d@sliit.lk

***Abstract* - The rapid rise of cybersecurity threats has led to the development of advanced security operations centers (SOCs) that can identify and respond to cyber-attacks in real-time. This research aims to design and implement a next-generation automated SOC using an automated ELK stack, threat hunting, intelligence, MITRE attack framework, and HIPAA compliance. The system will be evaluated using real-world scenarios to assess its effectiveness in enhancing SOC operations and threat identification. The study predicts that the next-generation automated SOC with an ELK stack will significantly improve cybersecurity operations by providing real-time network activity visibility, identifying, and analyzing threats, and automating response activities. The findings will emphasize the importance of incorporating new technologies into SOC operations and the need for continuous monitoring and enhancement. The study recommends further research into the integration of the ELK stack into automated SOC operations for better threat identification and response.**

Keywords: ELK, SOC, Kibana, Logstash, Automated MITRE Attack, Automated Threat Hunting, Automated Threat Intelligence, HIPAA Compliance, RBAC (Role Based Access Control), Machine Learning.

I. INTRODUCTION

Cybercriminals often focus their attention on healthcare providers and related institutions. The continuum of care results in a landscape that is convoluted and diverse in terms of the individuals, devices, apps, and procedures that comprise it. This landscape provides potential entry points for attackers into the network. A further tactic that attackers might use to carry out ransomware attacks is to threaten the interruption of essential life-saving utilities. The culmination of all these actions produces data that may be put to use to trace down attackers and stop them in their path. Indicators of data breach may be found across all sectors, but healthcare organizations want high-quality data that is tailored to their operating conditions in order to cut down on the amount of time it takes to discover and react to threats. Due to the sensitive nature of patient data, the healthcare business is a top target for the perpetration of cyberattacks. It is possible for patients, healthcare professionals, and healthcare organizations to face serious repercussions as a result of the theft, loss, or improper use of sensitive information. As a result, it is essential to have an efficient cybersecurity plan in order to safeguard patient data and stay in compliance with HIPAA regulations. An automated SOC can identify and react to potential dangers in real time, making it possible to take a complete and preventative approach to information security. The manual SOC technique that has been used in the past is no longer adequate due to the growing number of cyber threats and their increased complexity. An automated Security Operations Center (SOC) can analyze vast amounts of data, identify trends, and detect dangers that human analysts may overlook. This advantage over traditional SOCs allows for automation of mundane tasks like patch management, vulnerability scanning, and incident response, freeing security analysts to focus on more important responsibilities.

This leads to enhanced efficiency and efficacy in threat detection and response, reducing the risk of cyberattacks and data breaches. An automated SOC plays a crucial role in protecting patient data and maintaining HIPAA compliance. It enables real-time detection and response to cyber threats, minimizing the risk of data breaches and cyber assaults. Additionally, an automated SOC can help healthcare companies lower the cost of cybersecurity operations by automating mundane operations and combining threat intelligence, vulnerability management, and compliance management. This integration helps identify potential security concerns before they become a threat, minimizing the probability of data breaches and cyber assaults. The healthcare sector is increasingly targeted by sophisticated and persistent cyber-attacks, making the need for an automated SOC even more crucial. Advanced capabilities of automated SOC solutions, such as machine learning and artificial intelligence, can help organizations identify and respond proactively to complex threats. Overall, healthcare institutions must have an automated SOC to safeguard patient information and maintain HIPAA compliance. The healthcare industry requires an automated Security Operations Center (SOC) to identify vulnerabilities and weaknesses in defense mechanisms. The MITRE Attack framework enables SOC to conduct simulations of real-world attack scenarios, maintaining a competitive advantage over potential threats. This proactive approach strengthens existing security measures and enhances preparedness for incident response. Automated threat hunting helps identify sophisticated threats and malevolent actions within the healthcare network, evading conventional security measures. By analyzing network logs, traffic, and behavior patterns, SOC can detect and identify activities that deviate from the norm, potentially indicating concealed threats. The integration of automated threat intelligence into the Security Operations Center (SOC) enables swift and effective response to emerging threats, vulnerabilities, and attack tactics. This real-time knowledge improves SOCs' ability to anticipate and mitigate potential cyber-attacks. Automated threat intelligence feeds enhance contextual information, facilitating better decision-making and incident response. Compliance with HIPAA is essential for maintaining patient data confidentiality and integrity. The SOC plays a crucial role in protecting sensitive information by monitoring and implementing measures to prevent potential breaches. Proactive approach to unauthorized access and disclosure of sensitive data is crucial to prevent legal repercussions. SOCs, continuous monitoring, and safeguarding practices protect critical information integrity. Compliance frameworks uphold patient trust and regulatory standards. Role-Based Access Control (RBAC) enhances system security by implementing access controls aligned with specific roles and responsibilities. Role-Based Access Control (RBAC) in the Security Operations Center (SOC) helps mitigate risks of unauthorized access to sensitive data. By restricting access privileges based on roles and responsibilities, RBAC minimizes data breaches and enhances the overall security posture, safeguarding valuable data assets and aligning with research on data protection and patient confidentiality preservation.

Utilizing a web portal for our integrated cybersecurity system represents a forward-thinking approach to managing digital threats and ensuring regulatory compliance. By incorporating automated Security Information and Event Management (SIEM) with the MITRE ATT&CK framework, Threat Hunting, Threat Intelligence, and automated HIPAA compliance measures, our web portal offers a centralized and user-friendly interface. This allows security professionals to efficiently monitor, analyze, and respond to potential threats in real-time, streamlining incident detection and response processes. The web portal provides a holistic view of the organization's security posture, enabling quick decision-making and facilitating collaboration among cybersecurity teams. This intuitive platform not only enhances the efficiency of threat mitigation but also ensures seamless compliance with HIPAA regulations, safeguarding sensitive healthcare data.

II. RELATED WORK

In a blog post by Alparslan Akyildiz, the author analyzes cyber-attacks using ELK and models real-life APT (Advanced Persistent Threat) attacks in a lab setting. The search results don't say anything about the specifics of the study or what it found. But this blog post probably shows how ELK can be used for threat information and hunting. It also shows how ELK can be used to find and stop cyber-attacks.

Delgado's thesis suggests and evaluates The Elasticsearch Stack solution (ELK) as an adaptive solution for threat hunting. The ELK stack is an enterprise-grade store for logs and a search engine that lets you actively look for threats. The thesis looks at how well the ELK stack can gather, store, and analyze log data from different sources so that potential threats can be found and dealt with. The ELK stack's ability to work with a wide range of IT and security technologies is also emphasized. This helps companies get rid of blind spots and data silos. The conclusion of the thesis is that the ELK stack is a powerful tool for threat hunting, and groups that want to improve their ability to find threats and deal with them should use it.

Using the MITRE ATT&CK approach, TrustedSec offers a resource for making it easier to plan operational threat hunts. The MITRE ATT&CK model is a way to learn about and classify the tactics, techniques, and procedures (TTPs) of an enemy. The resource stresses how important it is to understand the MITRE ATT&CK model as a guide for putting together planned actions for threat hunting. It also shows how important it is to be proactive to find strange behavior quickly and test how well detection rules work. The resource suggests working with threat models to build, test, and improve methods for threat hunting. Overall, the resource shows how organizations can use the MITRE ATT&CK model to simplify planning for practical threat hunts and improve their ability to find threats and respond to them.

SourceForge compares the best SIEM software for nonprofits in 2023, including those with threat intelligence, MITRE ATT&CK framework implementation, and advanced features for taking down threats. ConnectWise SIEM is in the comparison because it is built with multiple tenants in mind and has the best threat data on the market. LogRhythm, which uses the MITRE ATT&CK framework to offer compliance modules, threat feeds, and security data, is also in the comparison. Also included in the comparison are Kloudle, SafeDNS, and phoenixNAP, which are all cloud-based security programs with advanced features for finding threats and other security features. Overall, the comparison shows what the best SIEM software choices for nonprofits will be in 2023, such as those with threat intelligence, MITRE

ATT&CK framework implementation, and advanced threat hunting features.

III. METHODOLOGY

Many phases make up the technique for automating ELK stack for a healthcare sector automated security operation center. The initial stage is to gather information from multiple sources (e.g., logs, network traffic, system activity, etc.). Agents, syslog, application programming interfaces, etc. are just a few of the technologies that may be used to gather the data. The next step is to import all this data into the ELK stack, a collection and analysis tool. Elasticsearch, Logstash, and Kibana form what is known as the ELK stack. Elasticsearch is used to index and store the data once it has been processed and transformed using Logstash. Kibana may be used to visualize data and do exploratory analyses. The system overview of the application is shown in the following Fig. 1.

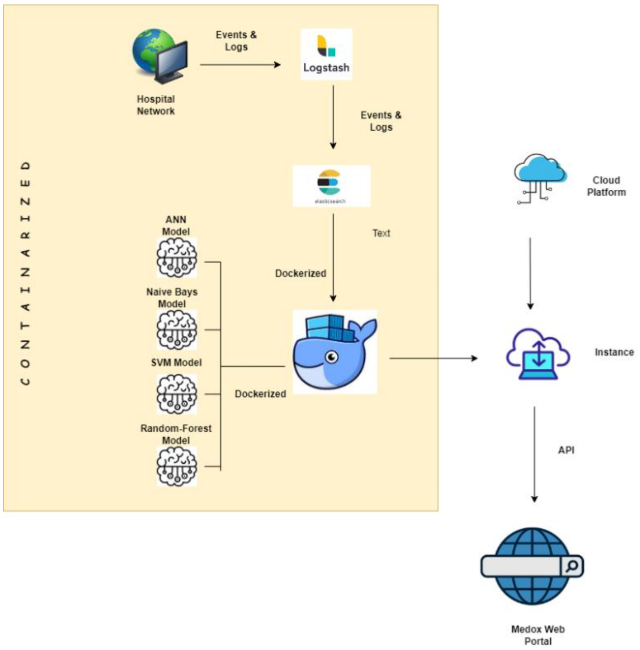

Figure 1: Overall System Diagram

In the methodology employed in this research project is a multifaceted approach designed to fortify the security operations within the healthcare domain. The foundation of this endeavor is established with the implementation of the Elastic Stack (ELK), consisting of Elasticsearch, Logstash, and Kibana. These components are containerized to facilitate cloud-based deployment, allowing for scalability and flexibility in handling healthcare data.

The ELK stack is meticulously configured to serve as a Security Information and Event Management (SIEM) system, purpose-built for analyzing the influx of Internet of Medical Things (IoMT) logs. This SIEM infrastructure serves as the backbone for the subsequent machine learning models, providing a comprehensive platform for log analysis and anomaly detection.

The core innovation of this research methodology lies in the integration of machine learning models, each tailored to address specific security challenges. The first of these models is an Artificial Neural Network (ANN), meticulously trained to function as an automated threat intelligence tool. This ANN model not only categorizes incoming log entries but also evaluates their severity, ensuring alignment with the stringent data protection standards outlined by the Health Insurance Portability and Accountability Act (HIPAA).

Complementing this, a Support Vector Machine (SVM) model is incorporated to tackle the intricacies of MITRE attack framework detection. Leveraging attributes such as IP addresses, device characteristics, log sources, user identities, and event identification codes, the SVM classifies incoming events as either malicious or legitimate. It does so with an emphasis on adherence to the MITRE framework, thereby providing advanced threat detection capabilities.

To further enhance the security posture, a Naive Bayes machine learning model is deployed. This model is purpose-built for automated threat hunting, focusing on the inspection of specific elements. These include Dynamic Link Library (DLL) files, service names, scheduled tasks, system processes, and CPU usage. The model provides a comprehensive assessment of the legitimacy of individual events, with a specific focus on IoMT devices and hospital equipment.

A crucial component of this research methodology is the development and configuration of a web portal. This portal serves as an integral communication bridge between the machine learning models and healthcare professionals and administrators. It is equipped with real-time alert generation capabilities, ensuring that anomalies and security incidents are conveyed promptly and accompanied by comprehensive details and contextual information.

Patient data privacy and categorization under the stringent provisions of HIPAA compliance are addressed through the application of a Random Forest machine learning model. The model stratifies data into categories of criticality, differentiating between critical, high, medium, and low priority classifications. This categorization helps maintain the integrity of patient data and ensure its adherence to the highest data protection standards.

All components and models are seamlessly integrated within a cloud-based environment. Each machine learning model is containerized using Docker technology, ensuring efficient deployment and accessibility. HTTP endpoints are established through Flask, allowing for seamless communication and interaction with these models. Docker containers housing these models are deployed on cloud instances, providing a robust and easily accessible system.

The research project culminates with a comprehensive evaluation and validation process, demonstrating consistent accuracy levels exceeding 97% across all machine learning models. This methodology represents a holistic approach to enhancing the security posture within healthcare operations, delivering data protection, compliance with HIPAA standards, and threat detection capabilities. It leverages technical innovation to enhance the practical usability of a Security Operations Center, ensuring that healthcare professionals can confidently safeguard sensitive patient data and maintain a secure healthcare ecosystem.

3.1 MITREAttack Framework

This study employs qualitative research methods due to their ability to facilitate idea development and in-depth understanding. The research involves gathering data from various sources, such as Google Scholar, and utilizing methods like interviews, focus groups, and questionnaires. The research questions aim to understand cyberattack patterns, countermeasures against attacks, and how the healthcare industry could adopt the MITRE ATT&CK framework. Results aim to demonstrate how the framework enhances healthcare system security by detailing attacker actions. Red teams use this framework to breach systems, while blue teams prepare defenses. Reliable secondary sources, including databases like Google Scholar, Microsoft Academic Search, and Base, provide accurate information. This study seeks to shed light on healthcare cybersecurity using qualitative research and the MITRE ATT&CK framework. Implementation of MITRE ATT&CK in healthcare: There are a few different ways that automated threat intelligence can be integrated with the ELK stack in a healthcare industry SOC:

- Network nodes, servers, apps, and the cloud are just some of the places from which data is gathered. A Security Information and Event Management tool in the ELK stack is responsible for collecting and storing this information.
- "Enrichment" of data occurs when it is supplemented with information from other places, such as threat intelligence feeds, vulnerability databases, or regulatory compliance mandates.
- To identify potential security issues, machine learning algorithms and automatic correlation procedures are applied to the augmented data.
- The severity and likelihood of a threat are both factored into a single score.
- Security analysts can quickly detect the most pressing threats thanks to a dashboard that displays the threat rating data.
- The identified threats are dealt with by means of automated response mechanisms, such as the blocking of an IP address or the quarantining of a device.
- The system is continuously assessed and improved to guarantee the precision of the threat detection algorithms, especially as new threat information sources become available.

By using this technology, analysts may quickly identify dangers and take appropriate action with minimum human intervention. It guarantees that medical facilities will be able to keep patient records and follow all relevant rules.[8]. Companies in the healthcare industry may find value in utilizing the MITRE ATT&CK architecture since it functions as a framework for attack mapping and analysis. By applying the MITRE ATT&CK paradigm, it is feasible to gain a deeper comprehension of the techniques that would be utilized to break into the systems of a healthcare company. This is important information. The data that was collected can be utilized by the healthcare industry to produce an MITRE ATT&CK architecture-based map of the malware attacks that are experienced most frequently.[9] After doing a thorough analysis of the data obtained, the researchers at MITRE came to the conclusion that they had built an independent Ransomware Resource for healthcare organizations and professionals.

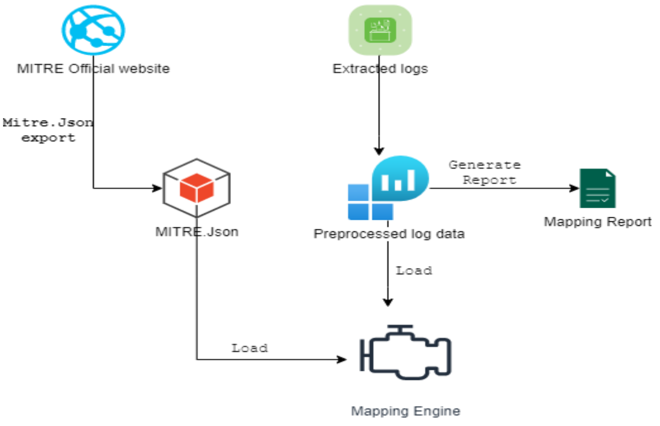

Figure 2: System Diagram Automated Mitre Attack Framework

Subsequently, a Support Vector Machine (SVM) model is integrated into the research methodology, specifically tailored to address the complexities posed by the MITRE attack framework. This SVM-based component is engineered to discern the subtleties of incoming security events and classify them as either malicious or legitimate. The criteria for making this classification are multifaceted, encompassing a meticulous analysis of attributes such as IP addresses, device characteristics, log sources, user identities, and event

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 299-306, November-2023
https://doi.org/10.47001/IRJIET/2023.711041

identification codes. The SVM's capacity to dissect these parameters enables it to make precise predictions regarding the nature of incoming events, safeguarding healthcare infrastructure against potential threats.

In conjunction with this, an advanced mitigation mechanism is established, harmonizing with the MITRE framework. Upon classification, the SVM-equipped system instantaneously initiates an appropriate mitigation strategy, assuring timely and effective responses to security incidents. In the event of malicious activities or threat indicators being identified, the system takes pre-defined actions to mitigate these risks. These actions are orchestrated to align seamlessly with the MITRE framework, reinforcing the security posture with actions rooted in industry-standard practices.

To enable the seamless interaction between the SVM model and the healthcare ecosystem, an HTTP endpoint is created using Flask, a micro web framework. This Flask-based interface acts as a vital communication conduit, enabling healthcare professionals and administrators to transmit data and receive predictive results. It ensures a dynamic and real-time interface for both the deployment of the SVM model and the receipt of mitigation strategies, thus augmenting the overall security operations within the healthcare domain.

This SVM component serves as a cornerstone in bolstering the security operations within healthcare and adheres to the stringent regulations of the MITRE framework. Its real-time predictive capabilities are underpinned by the technical precision of SVM, ensuring that the security of patient data and healthcare infrastructure remains uncompromised.

3.2 Automated Threat Hunting

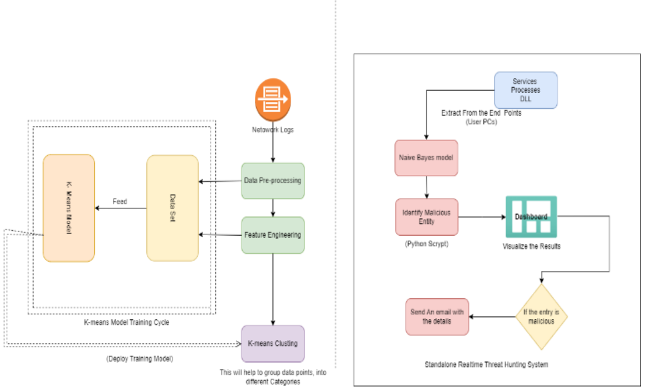
Network Logs
Data Pre-processing
Feature Engineering
Data Set
Feed
K- Means Model
K-means Model Training Cycle
(Deploy Training Model)
K-means Clusting
This will help to group data points, into different Categories
Services Processes DLL
Extract From the End Points (User PCs)
Naive Bayes model
Identify Malicious Entity
(Python Scrypt)
Dashboard
Visualize the Results
If the entry is malicious
Send An email with the details
Standalone Realtime Threat Hunting System

Figure 3: System diagram Automated threat Hunting

This research presents a novel approach to hospital network security by utilizing the K-means clustering method and the Naive Bayes model together to achieve advanced threat identification. Using the K-means algorithm, the system effectively groups network logs into clusters, finding commonalities between data points and extracting insightful information from endpoints for further examination. Potential threats are quickly discovered and shown on a dynamic dashboard that offers a full picture of the network's security state by comparing this data with known harmful patterns.

By fusing the advantages of human knowledge with machine learning, this integrated method provides a proactive cybersecurity plan. Logs are intelligently grouped into clusters using the K-means algorithm, which reveals patterns that were previously unknown. The Naive Bayes model improves the system's prediction power. The system's core module contributes to the process of overall threat identification by extracting comprehensive endpoint information. The dynamic dashboard enhances cybersecurity professionals' threat visibility by seamlessly integrating endpoint analysis and machine learning forecasts.

The approach emphasizes how crucial it is to create and refine datasets that are especially suited to the subtleties of healthcare cybersecurity. The combination of domain-specific expertise and computing power yields a novel method that successfully tackles the particular difficulties presented by healthcare technology. The solution's core extraction mechanism converts complex endpoint activity into illuminating stories that aid in a better comprehension of possible security risks.

This study demonstrates how to greatly improve network security through the use of both K-means clustering and the Naive Bayes model in log analysis. Importing necessary libraries for data administration, visualization, and mathematical operations includes numpy, matplotlib.pyplot, and pandas. The severity and event count properties of the dataset are loaded and processed. The Elbow Method is used to visualize the within-cluster sum of squares and use iterative K-means applications to discover the ideal cluster count. Next, K-means is used to forecast cluster assignments. The resulting scatter plots show clusters clearly, colored according to the assignment, with yellow centroids emphasizing the cluster centers. The 'Cluster' column is incorporated into the dataset as a point of reference, providing an all-encompassing method that effectively classifies logs and enhances threat detection and security protocols.

3.3Automated Threat Intelligence

Advanced threat intelligence systems depend on their data collection mechanism's strength and reliability. The Automated Threat Intelligence System uses a wide range of sources to ensure timely and relevant threat data acquisition, forming a robust and adaptable detection framework.

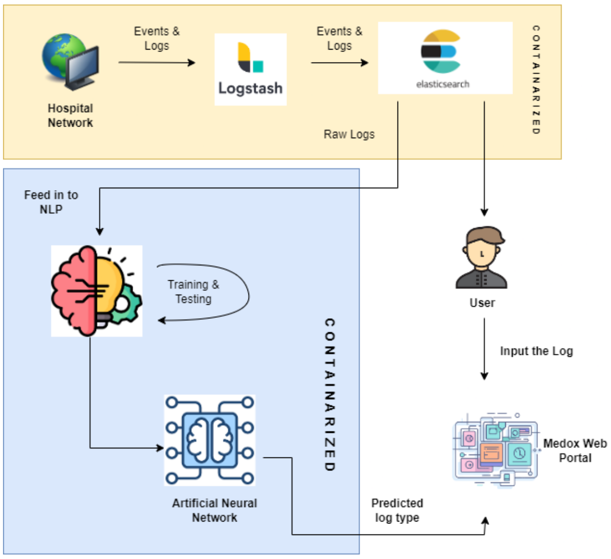

Figure 4: System Diagram Automated Threat Intelligence

In this research, a meticulous and complete approach is used, and it is optimized to construct an advanced automated threat intelligence system that is especially customized to the needs of healthcare security. Complexity is going to be used as the approach is comprised of a number of separate stages, each of which plays a key part in the larger objective of enhancing threat detection and categorization. For automated threat intelligence system, used ANN model. The integration of an ANN model in the script enhances the accuracy, flexibility, and automation of log data classification. It leverages the strengths of ANNs to streamline the log analysis process and provide users with reliable and efficient log categorization. First, when combined, provide a thorough answer for the pre-trained Artificial Neural Network (ANN) model used in the categorization of log data. The ANN model in this instance focuses on setting up the foundation for log data processing, including text cleaning, data preprocessing, model loading, and classification. It downloads stopwords for natural language processing, imports necessary libraries, and effectively manages the transformation and cleaning of log data. The script loads the pre-trained models, which include the count vectorizer for text-to-numerical conversion and the ANN model for log type prediction. The ANN model is an effective tool for classifying batch log data as it predicts log kinds and shows the findings after thorough text preparation. Then, by easily integrating with the first script, improves user engagement and real-time log data categorization. Users are able to directly enter log data and go through the identical ANN-based categorization, data preparation, and prediction presentation steps. It acts as a user-friendly interface, allowing users to communicate with the ANN model. It is especially helpful for those who want to get instant log type predictions. When combined, these scripts provide a flexible and intuitive framework for classifying log data, simplifying the application of the ANN model, and guaranteeing that the requirements for processing log data in batches and in real-time are satisfied.

3.4 Automated HIPAA Compliance

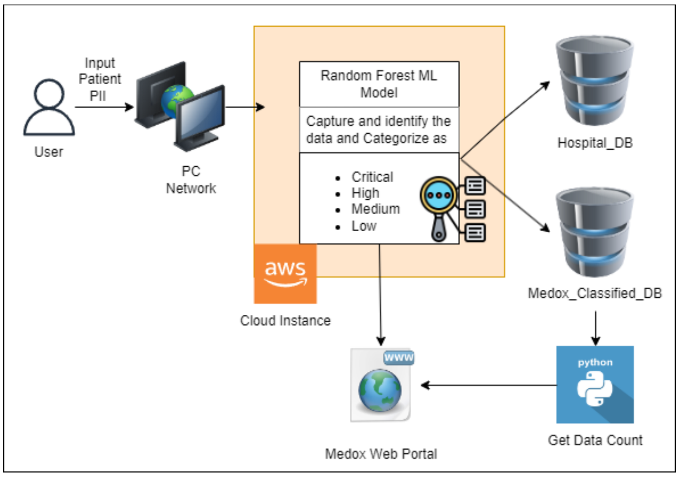

Figure 5: System Diagram Automated HIPAA Compliance

In this research paper, our focus is on data classification based on HIPAA compliance, with a primary emphasis on safeguarding patient data privacy. We have constructed a dataset encompassing various patient information, including the patient's ID number, name, age, email, date of birth, address, gender, blood type, allergies, diagnosis, and vaccination history. To categorize this data in terms of criticality, we employed a Random Forest machine learning model, which stratified the data into critical, high, medium, and low priority classifications. Critical data includes medical-related information and the patient's ID number, while high priority data encompasses email addresses and home addresses. Medium priority data comprises names and blood types, and low priority data includes date of birth, patient ID, and gender. Our approach is flexible, allowing the addition of more data types as per client requirements. The trained model is stored within the ELK stack, and we created an HTTP endpoint using Flask. A Docker container was built and deployed on an AWS EC2 instance, providing an API to our Medox web portal. Within the Medox web portal, we introduced a dedicated "HIPAA" tab, offering various functionalities for users. The webpage presents a Data Analysis option and a HIPAA Compliance Report feature. It provides a breakdown of critical, high, medium, and low data counts stored in the database, making it easier for hospitals to monitor data collection and classification. Our solution aims to simplify HIPAA compliance for healthcare staff with limited knowledge in this domain. In the Data Analysis section, users can enter data types and assess their severity classification. The HIPAA Compliance Report allows users to select a specific date range, generating data counts in various categories and presenting results through summary tables and pie charts for senior management. Furthermore, users have the option to download the compliance report to facilitate communication with technical experts, thus enabling the implementation of appropriate security measures to protect patient data privacy.

IV. RESULTS AND DISCUSSIONS

The deployment of a fully automated Security Operations Center (SOC) tailored for the healthcare industry has yielded substantial benefits. Incorporating automated threat hunting, threat intelligence, MITRE ATT&CK framework integration, and compliance solutions has revolutionized cybersecurity approaches. The SOC can now proactively manage emerging risks through automated threat hunting. The MITRE ATT&CK framework enhances incident responses by providing insights into adversary tactics. Automated compliance solutions ensure adherence to strict regulations like HIPAA. Real-time data analysis reduces response times to potential threats, bolstering security and patient data protection. Benefits include improved threat detection and response, proactive defense, efficiency gains, compliance adherence, resource optimization, continuous monitoring, adaptability, reduced human error, cost efficiency, and innovation potential. This innovative SOC, guided by skilled cybersecurity personnel, represents a crucial advancement in fortifying digital landscapes. Challenges include integration complexities, real-time data processing, MITRE ATT&CK alignment, sector-specific compliance, human-machine collaboration, adaptability, and resource allocation. Success relies on careful planning and collaboration between automation and human expertise.

V. CONCLUSION

Future iterations of this system may be able to save expenses by making better use of efficient technologies, such as by decreasing the labor cost of components like SOC and hardware. We want to deploy in Sri Lankan hospitals since there is a lack of necessary infrastructure in the present system. In addition, consumers will have access to live, round-the-clock help. The potential of this unified approach to bolster detection and reaction times, simplify threat hunting, and guarantee conformity to vital compliance requirements like HIPAA has been established. The system's machine learning algorithms, its threat intelligence database, and its automatic reaction mechanisms all need further development as technology progresses. Further strengthening the system's accuracy, efficacy, and agility in the face of developing threats will need continuing cooperation with industry experts and input from cybersecurity specialists. In the end, this automated SIEM is likely to play a crucial role in the coming years in reinforcing digital landscapes and protecting critical information. In conclusion, our web portal streamlines cybersecurity management by integrating automated SIEM, MITRE ATT&CK, Threat Hunting, Threat Intelligence, and HIPAA compliance. This user-friendly interface empowers security professionals to monitor and respond to threats in real-time, fostering quick decision-making and collaboration. The platform not only enhances threat mitigation efficiency but also ensures seamless compliance with HIPAA regulations, safeguarding sensitive healthcare data.

ACKNOWLEDGEMENT

We owe a great debt of gratitude to the natural world, which had a hand in our fortuitous birth and compels us to pursue our motivations with unwavering dedication. By agreeing to serve as our research supervisor, Mr. Kanishka Yapa, and for agreeing to serve as our co-supervisor, Mr. Uditha Darmakeerthi, respectively, our sincerest appreciation is extended.

REFERENCES

[1] "Implementing MITRE ATT&CK – Innovate Cybersecurity | Threat Advisory, News, and Events." https://innovatecybersecurity.com/news/implementing-mitre-attack/ (accessed Mar. 20, 2023).

[2] R. Al-Shaer, J. M. Spring, and E. Christou, "Learning the Associations of MITRE ATT&CK Adversarial Techniques," Apr. 2020, Accessed: Mar. 20, 2023. [Online]. Available: https://www.researchgate.net/publication/341149123_Learning_the_Associations_of _MITRE_ATTCK_Adversarial_Techniques

[3] "Benefits of a Continuous SOC | Fortified Health Security." https://fortifiedhealthsecurity.com/blog/how-a-continuous-soc-can-help-healthcarefacilities-avoid-data-loss/ (accessed Mar. 20, 2023).

[4] "Basic Threat Hunting Using the MITRE ATT&K Framework." https://www.linkedin.com/pulse/basic-threat-hunting-using-mitre-attk-frameworkalex-hardt (accessed Mar. 20, 2023).

[5] A.Adedoyin and H. Teymourlouei, "Methods for automating threat hunting and response," in 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2021.

[6] M. Arafune et al., "Design and development of automated threat hunting in industrial control systems," in 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2022.

[7] A.J. Horta Neto and A. Fernandes Pereira dos Santos, "Cyber threat hunting through automated hypothesis

and multi-criteria decision making," in 2020 IEEE International Conference on Big Data (Big Data), 2020.

[8] S. Moza A L and Anupriya, "Automated threat hunting using ELK stack - A case study," Indian J. Comput. Sci. Eng., vol. 10, no. 5, pp. 118–127, 2019.

[9] A.Yazdinejad, M. Kazemi, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "An ensemble deep learning model for cyber threat hunting in industrial internet of things," Digit. Commun. Netw., vol. 9, no. 1, pp. 101–110, 2023.

[10] M. Guarascio, N. Cassavia, F. S. Pisani, and G. Manco, "Boosting cyber-threat intelligence via collaborative intrusion detection," Future Gener. Comput. Syst., vol. 135, pp. 30–43, 2022

[11] Z.-X. Li, Y.-J. Li, Y.-W. Liu, C. Liu, and N.-X. Zhou, "K-CTIAA: Automatic analysis of cyber threat intelligence based on a knowledge graph," Symmetry (Basel), vol. 15, no. 2, p. 337, 2023

[12] K. M. Khan and Y. Bai, "Automatic verification of health regulatory compliance in cloud computing," IEEE Xplore, Oct. 01, 2013. https://ieeexplore.ieee.org/abstract/document/6720770 (accessed Mar. 28, 2023).

[13] E. B. Sloane and C. C. Carey, "Using Standards to Automate Electronic Health Records (EHRs) and to Create Integrated Healthcare Enterprises," IEEE Xplore, Aug. 01, 2007. https://ieeexplore.ieee.org/abstract/document/4353765/ (accessed Mar. 28, 2023).

[14] M. Zineddine, "Automated healthcare information privacy and security: UAE case," IEEE Xplore, Dec. 01, 2011. https://ieeexplore.ieee.org/abstract/document/6148404 (accessed Mar. 28, 2023).

[15] A.Mahindrakar and K. P. Joshi, "Automating GDPR Compliance using Policy Integrated Blockchain," 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), May 2020, doi: https://doi.org/10.1109/bigdatasecurity-hpsc-ids49724.2020.00026.

AUTHORS BIOGRAPHY

Abeysinghe A.M.S.B.,
Undergraduate at SLIIT | Sri Lanka Institute of Information Technology, Specialized in Cyber Security.

De Zoysa M.T.R.,
Undergraduate at SLIIT | Sri Lanka Institute of Information Technology, Specialized in Cyber Security.

Samuditha K.M.Y.,
Undergraduate at SLIIT | Sri Lanka Institute of Information Technology, Specialized in Cyber Security.

Dissanayake D.J.D.H.T.,
Undergraduate at SLIIT | Sri Lanka Institute of Information Technology, Specialized in Cyber Security.

Kanishka Yapa,
Lecturer at SLIIT | Sri Lanka Institute of Information Technology, Faculty of Computing | Computer Systems Engineering.

Uditha Dharmkeerthi,
Lecturer at SLIIT | Sri Lanka Institute of Information Technology, Faculty of Computing | Computer Systems Engineering.

Citation of this Article:

Abeysinghe A.M.S.B., De Zoysa M.T.R., Samuditha K.M.Y., Dissanayake D.J.D.H.T., Kanishka Yapa, Uditha Dharmkeerthi, "Security Operation Center for Healthcare Sector" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 299-306, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711041

****