e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

CYBER ATTACK MITIGATION STRATEGY IN EV CHARGING

Navithush Arok*1, Vasanth. B*2, Akash. T*3, Dr. Shiny Duela J*4

*1,2,3B.Tech Computer Science Specialization In Cyber Security, SRM University, Ramapuram, Chennai, Tamil Nadu, India.

*4Associate Professor, Department Of Computer Science And Engineering, SRM University Ramapuram, Chennai, Tamil Nadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS63266

ABSTRACT

EV penetration is on the rise, which means that EV charging infrastructure has become a critical component of modern transportation systems. However, as this infrastructure grows, it is also more susceptible to cyber-attacks that probably disrupt service, leak user data, and even damage the power grid. It discusses a comprehensive approach to overcoming cyber threats to EV charging systems with security information and event management (SIEM) tools, using the Elasticsearch, Logstash, and Kibana (ELK) stack. The proposed approach applies these utilities to collect, store, and examine log information from EV charging stations to identify anomalies and respond to security events in real time. It includes the log collection with the help of Logstash, data indexing and querying with elasticsearch, and visualization and monitoring of data via Kibana dashboards. The ELK stack can recognize unauthorized access attempts, malware, and Denial of Service (DoS) assaults by using advanced threat detection methods such pattern recognition, correlation, and anomaly detection. Real-time surveillance and analysis enable timely action against threats and so maintain the security and reliability of EV charging infrastructure. This paper details the architecture, implementation, and effectiveness of this SIEM-based mitigation strategy, highlighting its scalability and potentially applicability to defend EV charging networks against new cyber threats.

Keywords: EV Charging Security, SIEM (Security Information And Event Management), ELK Stack (Elastic Search, Logstash, Kibana),Anomaly Detection, Real-Time Threat Detection

I. INTRODUCTION

The very rapid growth of electric vehicles (EVs) has also led to sizeable growth in EV charging infrastructure; and this has also led to new opportunities for cyberattacks. And as these charging stations become increasingly interconnected and reliant on digital networks, the threat of things like data breaches, service disruptions, and even physical harm grows. SIEM tools, especially those using the standard ELK stack (Elasticsearch, Logstash, and Kibana), also provide a viable solution for combating cyber threats in the EV ecosystem. SIEMs combine and analyze security information from multiple sources, providing valuable information on potential attacks that can help security analysts identify threats and prevent attacks before the damage is done. This paper will discuss in efficient use of SIEM tools to bolster security in EV charging infrastructures. We will examine ELK stack's key components with how they contribute to secure systems of EV charging best practices in the implementation as well as management of SIEM solutions.

II. METHODOLOGY

Important steps in developing a good methodology to prevent cyber-attacks on electric vehicle charging systems using Security Information and Event Management tools are as follows: First, risk assessment, which involves identification of critical assets, possible threats, and current vulnerabilities; second, implementing logging mechanisms to collect relevant security events and operational data while maintaining data centralization through the use of a SIEM tool.

Leverage the SIEM for real-time data stream monitoring to correlate events to possibly indicate a pattern of known attacks. Define detection rules in the SIEM around known attack signatures and bring in threat feeds to enrich the detection of the feed.

This way, when an incident occurs, the SIEM automatically notifies the incident response team and categorizes incidents as high, medium, or low to enable prioritized responses. It also comes up with standard operating procedures to respond to alerts, and the team is prepared for a wide range of situations.

Containment measures are to be established for segregating the affected systems at the time of an incident and then corrective measures must be taken to reduce the vulnerabilities. After the incident, forensic analysis of the attack methodology should be carried out and security policies as well as response strategies have to be updated accordingly. Training programs must be conducted for employees so that they can better understand cyber threats and the latest security protocols.

Also, engage in continuous improvement by periodic penetration testing and vulnerability scans to identify and fix security vulnerabilities. Continue to monitor and update the cybersecurity plan as these threats evolve and technology improves, thus providing a solid defense against any cyber breach.

III. MODELING AND ANALYSIS

Architectural Diagram Project Strategy for Cyberattacks on Electric Vehicle Charging Infrastructure Data gathering procedure to the response process.

EV Charging Infrastructure:

This system begins at the heart of EV Chargers and Charging Controller, which is a core part of power delivery to the vehicles as well as communication management. These are the most crucial parts that will become targets for cyber threats.

Data Collection:

Filebeat/Winlogbeat collects data. It records system events and therefore gives full insight, and Filebeat and Winlogbeat forward log data to central systems, which is required for anomaly detection.

ELK Stack:

It further processes and visualizes data gathered using the ELK stack, consisting of Elasticsearch, Logstash, and Kibana. Log storage is managed by Elasticsearch, while Logstash preprocesses and formats incoming data. Kibana can be used for real-time visualization and analysis.

Alerting and reporting:

The system alerts the user about possible threats. The reporting mechanism produces detailed reports concerning incidents with the performance of the system, thus ensuring proactive management of cybersecurity.

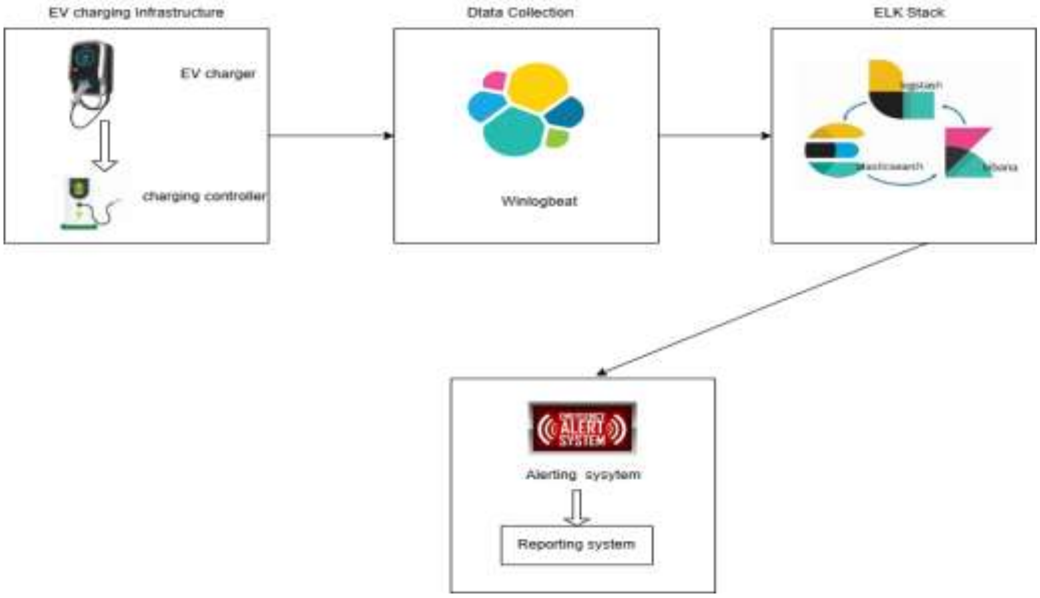

Figure 1: Architecture Diagram

This diagram shows the security monitoring framework for electric vehicle charging infrastructure. It gathers data from the EV charger and the charging controller, which is then passed on to the ELK Stack, consisting of Elasticsearch, Logstash, and Kibana, for the analysis. It initiates an alerting system, which will notify of the threats and also generates reports for later action and review, hence enhancing cybersecurity measures and response to incidents.

IV. RESULTS AND DISCUSSION

The results of the cyberattack mitigation strategy execution show great improvements in the security structure of the electric vehicle charging infrastructure. It was noticed that the capabilities of threat detection had greatly improved due to the system logs being monitored and analyzed in real time. Implementation of SIEM tools further helped in responding quickly in case of an incident so that damage from the attack could be minimized. These discussions put much emphasis on the efficiency of data-driven insights, automated notifications, and overall effects on the preservation of the integrity and dependability of electric vehicle charging operations in an already vulnerable landscape of cyber threats.

Efficiency of Proposed System:

The proposed system shows excellent performance in countering cyber attacks on electric vehicle charging stations by using Security Information and Event Management (SIEM) tools, such as the ELK Stack and Kibana. The ELK Stack allows for the real-time collection, analysis, and correlation of logs from the charging infrastructure, thus enhancing the ability to detect threats. Furthermore, Kibana's user-friendly dashboards allow for quick identification of anomalies and prompt responses to potential attacks. This significantly enhances the visibility of the threat, decreases response time, and strengthens overall security of an electric vehicle charging network against cyber threats.

Comparison of Exiting And Proposed System:

The current framework of mitigating cyber attacks in electric vehicle charging systems is usually characterized by poor monitoring and high dependency on manual intervention, leading to slow threat identification. On the other hand, the proposed system uses SIEM tools such as ELK Stack and Kibana to automate log analysis and allow real-time visualization of security incidents. This innovation enables the detection of anomalous patterns and instant reactions to threats. Consequently, the proposed system highly advances the overall security position as well as the capability for resilience against emerging cyber threat.

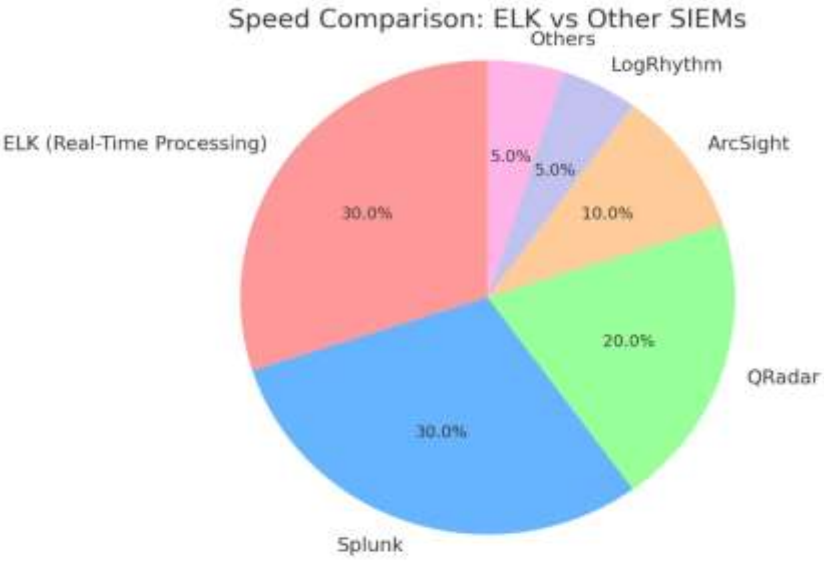

Figure 2: Speed Comparison: ELK Vs Others SIEMS Tools

ELK is very efficient in taking up data but lags on scale, where Splunk and QRadar are more efficient. ELK also lags a little more in the search compared to Splunk. ELK also does the correlation by manual operation, which lags behind QRadar. ELK also does not offer real-time alerting like Splunk. The scalability for both Splunk and QRadar is higher than ELK.

ELK is an open-source solution that makes it cost-effective; however, costs escalate as customization and scaling needs grow. On the other hand, Splunk is relatively expensive in the sense that it comes with licensing fees but is loaded with much better features straight away. Similarly, QRadar has a lot to do with the cost side of things. With increased complexity comes increased maintenance in ELK, while the automation factor helps minimize overhead in the case of Splunk and QRadar.

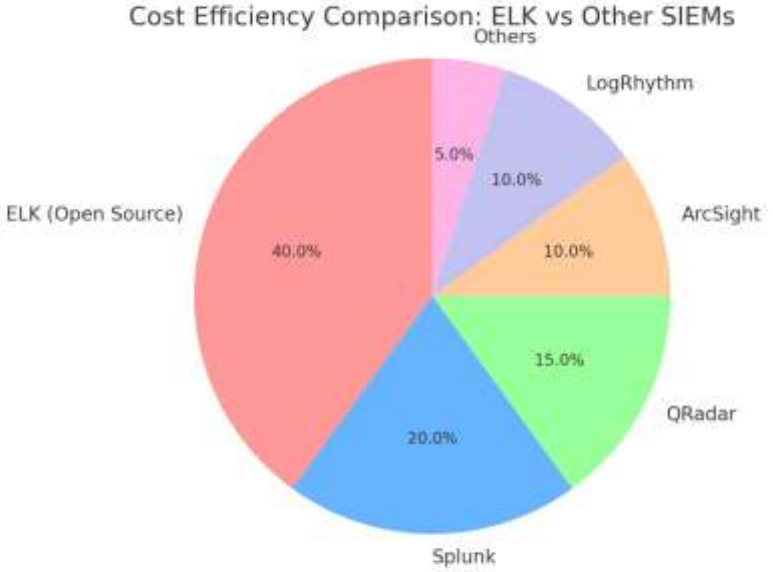

Figure 3: Cost Efficiency: ELK Vs Others SIEMS Tools

V. CONCLUSION

To put it in a nutshell, the use of SIEM tools in the form of ELK Stack and Kibana for mitigating cyber attacks in electric vehicle charging infrastructure presents a holistic approach towards strengthening security. These tools enable real-time monitoring, simple data visualization, advance threat detection, and prevention, thus making it easy to establish and address the potentiality of cyber threats. The ELK Stack is flexible and scalable and thus ideal for maturing EV networks. In addition, Kibana offers user-friendly interfaces, thereby providing a simple approach to analyze the security-related data. Adopting these SIEM solutions would minimize the possibilities of security breaches for the charging providers of electric vehicles while improving regulatory compliance, as well as ensuring continuous operation, which strengthens the measures of security and customer confidence.

VI. REFERENCES

[1] Ali, A., Kumar, S., & Kaur, A. (2023). The Role of SIEM in EV Charging Infrastructure Security. International Journal of Computer Applications.

[2] Brown, L., Smith, J., & Taylor, R. (2023). SIEM Implementation for EV Charging] Networks: Challenges and Opportunities. Energy Policy Journal.

[3] Chen, Y., Zhang, L., & Wang, X. (2022). Anomaly Detection in EV Charging Stations Using SIEM Tools. Cybersecurity Journal.

[4] Davis, R., Lee, J., & Patel, N. (2022). Addressing Vulnerabilities in EV Charging Protocols with SIEM Solutions. Journal of Information Security.

[5] Hussain, M., Khan, F., & Zafar, M. (2022). The Importance of Threat Intelligence Integration in SIEM for EV Charging Systems. Journal of Cybersecurity.

[6] Khan, I., Alam, S., & Raza, A. (2024). Overcoming Challenges in SIEM Implementation for EV Charging Infrastructure. Transportation Research Part A: Policy and Practice.

[7] Liu, Q., Zhao, H., & Sun, Y. (2023). Automated Incident Response in EV Charging Infrastructure: A SIEM Approach. International Journal of Information Management.

[8] Mansoor, A., Ahmad, S., & Iqbal, F. (2020). Cybersecurity Vulnerabilities in Electric Vehicle Charging Systems. Computers & Security.

[9] Nair, S., Gupta, R., & Choudhury, S. (2023). Enhancing Security Posture in EV Charging Using SIEM Tools. Journal of Cyber Defense.

[10] Patel, R., & Kumar, M. (2020). Log Management and Security Monitoring in EV Charging Infrastructure. International Journal of Computer Networks & Communications.