ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 2 Issue 1 March 2022 / Page No: 147-156
Paper Id: JETA-V2I1P117 / Doi: 10.56472/25832646/JETA-V2I1P117

Original Article

Bridging the Gap: Analyzing Emerging Threats in SAP Cybersecurity for Enterprise Landscapes

Kalam Kiran Kumar Reddy[1], Gunupati Kamalakar[2]
[1]*SAP Architect, India.*
[2]*Senior Vice President, India.*

Received Date: 08 January 2022 Revised Date: 05 February 2022 Accepted Date: 01 March 2022

Abstract*: SAP and other enterprise resource planning (ERP) systems have become prominent for integration into organizations following the era of digital transformation. SAP environments are mission critical systems and they attract elevated levels of cybersecurity threats that leverage on misconfigurations, interface, and other customizations. Therefore this paper aims at filling this gap by identifying new threats, implementation analysis and providing the appropriate mitigation measures in SAP landscapes IT security. We consider threats as unauthorized access, code injection, and ransomware attacks and focus on their operational and financial consequences. Furthermore, we assess the potential of new and advanced solutions like threat detection on the base of artificial intelligence and blockchain-based data protection in the context of SAP cybersecurity models. In this paper, we utilize theoretical and empirical approaches, correlate case studies and threats and use them to develop an ideal SAP cybersecurity model. The findings clearly indicate reduced vulnerability exposure levels and the effectiveness against complex threats. Risk management and security on enterprise SAP landscapes are a critical matter of concern for enterprises, and this paper concludes by arguing for an active approach to threat mitigation, as well as constant vigilance.*

Keywords: *SAP cybersecurity, Emerging threats, Enterprise landscapes, AI-Driven detection, Landscapes.*

I. INTRODUCTION

A. Overview of SAP in Enterprise Landscapes

SAP means Systems Applications & Products in Data Processing, a leading ERP software company that provides end-to-end applications from different business sectors to reduce complexities and increase productivity. SAP enables the strategic coordination of critical organizational activities of finance, procurement, human resources, and customer relationship management to drive organisational decision making and value addition for competitiveness. [1-4] It is an indispensable tool for large organisations globally because it provides an efficient means of consolidating important information and streamlining tasks across functions and divisions. This makes it, at the same time, the most widely used software and the most attractive for hackers. As the paper names dozens of data that can be retrieved or manipulated through SAP, it becomes clear that these systems demand strict security measures protecting them from unauthorized access. SAP cyber risks may result in disastrous results like data leakage, financial scams, production breakdowns, and customer trust deception, indicating the need to develop unique and preventive security measures.

B. Importance of Bridging the Cybersecurity

The significance of having a strong information control system in the contemporary business environment cannot be overemphasized, particularly considering the ever-growing importance of enterprise systems such as SAP. Addressing the cybersecurity divide is imperative to safeguarding critical corporate information and maintaining business function, compliance, and public confidence. There is an increasing divide between traditional forms of security and the increasingly complex forms of threats, stressing the need for better and SAP-specific security. Some reasons why it is essential to link this gap listed below are;

a) Protection of Sensitive Business Data:

SAP systems contain essential business information such as financial, customer and intellectual property information. In such an environment, a breach can cause a loss, theft or manipulation that can have severe implications on the company in terms of financial losses as well as loss of reputation. The two close the cybersecurity divide and protect against such threats while preserving business credibility and sensitive information.

b) Mitigating the Impact of Sophisticated Cyber Threats:

The new generation of Cyber threats is relatively aggressive compared to traditional threats like APTs and ransomware, and other advanced tactics outpace the traditional forms of security. New technologies like AI and BlockChain improve real-time threat detection when handling these complex attacks in the new age. Mitigating cybersecurity risk improves protection and reduces the effects of more advanced threats on SAP systems.

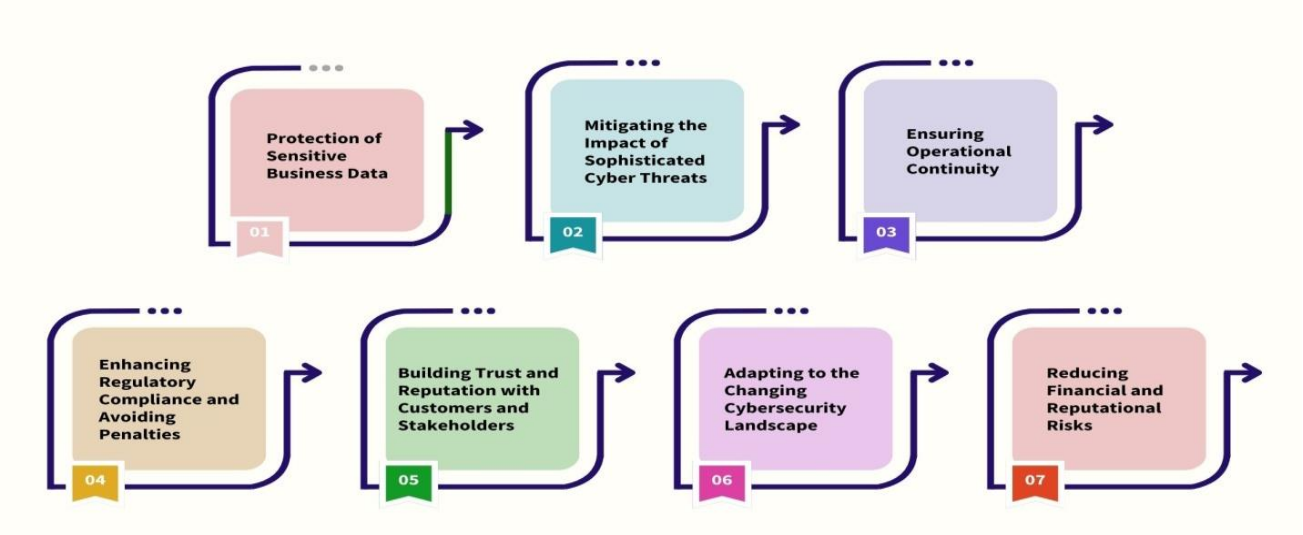

Figure 1: Importance of Bridging the Cybersecurity

c) Ensuring Operational Continuity:

SAP system disruptions due to cyberattacks can inhibit critical organizational processes such as financial transitioning, supply chain management, and even people management processes. Thus, closing the cybersecurity gap will enable the business to put in place measures that help with fast detection and response to threats to reduce the time taken. This means that SAP systems are not stopped when they are potentially vulnerable to cyber threats.

d) Enhancing Regulatory Compliance and Avoiding Penalties:

Much as organizations need to maintain the highest standards of compliance to ensure competitive advantage, there are legal requirements that organizations have to meet to avoid legal consequences in the form of fines, especially when handling customer data as per GDPR or patient data as per HIPAA, or any financial data as per SOX. Measures and frameworks exclusive to SAP guarantee that companies adhere to standard compliance and data protection regulations. Moving the cybersecurity gap minimizes non-conformity risks, resulting in hefty fines and adverse reports.

e) Building Trust and Reputation with Customers and Stakeholders:

Thus, in the modern world of big data, customers and other stakeholders are interested in how an organization defends their data. The exposure of an SAP system to a cyber risk means an organization's reputation and customer trust will be severely impacted. By closing the cybersecurity gap, business organizations show their preparedness to protect the data and, in the process, build trustful relationships with the customers.

f) Adapting to the Changing Cybersecurity Landscape:

Since threats in cyberspace are dynamic, there is a need to incorporate new security solutions such as AI and Blockchain into the security model. These technologies can be improved with new vectors unhinderedly because threats are not static. Curtain Raiser's cybersecurity gap enables businesses to cope with evolving threats and ensure that SAP systems are protected sufficiently.

g) Reducing Financial and Reputational Risks:

Cybercrime costs businesses money through ransoms, legal suits and other losses from disrupting their everyday operations. In addition, it can also have negative effects, such as compromising an organisation's image, resulting in a loss of customer confidence and market share. By closing the cybersecurity gap, businesses protect themselves from the breaches and, therefore, minimize the losses of different types of capital – monetary and reputational- which guarantee a stable industry development.

C. Cybersecurity Challenges In SAP Systems

a) Weak Authentication and Authorization Mechanisms:

A major cybersecurity threat in SAP systems is the lack of proper authentication and authorization processes. [5,6] Too often, SAP landscapes are structured with ubiquitous accessing profiles, meaning an SAP user ID encompassing many authorizations must be used. Thus, a security disaster is created if the situation is not tackled. Weak password creation and management policies, the lack of MFA, and undefined or weak roles and permissions allow the unauthorized entry of individuals into areas or functions that they should not be in or performing the wrong ways. The author concluded that these weak mechanisms can be exploited by attackers and used to elevate their privileges and navigate around security measures to gain access to such important business processes. By so doing, it becomes very critical for organizations to employ highly secured policies for IAM solutions, particularly with regard to user access restrictions to organizational resources based on least privilege, in addition to enforcement of strong user authentication mechanisms.

b) Insecure Configurations and Patch Management Challenges:

These systems are typically extensively built to suit organizational requirements, creating the risk of having insecure configurations and inadequate control of patches. Human mistakes in adjusting the system settings, security controls or network infrastructure elements can lead to the formation of weaknesses that will be useful to the attackers. Another complexity is that SAP environments can have some old versions of software or unprotected security holes that are not removed promptly because of weak patching. These vulnerabilities are a point of attack by cybercriminals with the possibility of auctioning exploits like the buffer overflow attack or privilege escalation. These are some of the ways in which patch management practice is used to counter these vulnerabilities, including ensuring that security patches and updates are released quickly and that system configurations are critiqued and made secure from possible threats.

c) Third-Party Integrations with Insufficient Security Protocols:

Most third-party applications, cloud services, and external partners are connected to the SAP systems to automate business processes. However, these third-party integrations can considerably expose the CIs if their security is not adequately improved. Very often, many of these external systems might not have adequate security controls as have been implemented in the SAP environment, or they could not follow industry best practices on data encryption or authentication. Third-party protection lapses can also present openings for wrongdoers to gain unauthorized access to an organization's system or acquire vital information. Due to these risks, organizations that incorporate third-party vendors need to implement security controls to ensure that these vendors embrace security policies that protect data and follow strong authentication techniques for communicating with the third-party system.

Figure 2: Cybersecurity Challenges in SAP Systems

II. LITERATURE SURVEY

A. SAP Security Vulnerabilities

SAP systems are important in organizations since they control important business processes and data. However, a large number of research studies have shown that critical weak linkages exist in these systems. [7-10] There are many risks associated with RFCs, which are common ways to enable communication between various SAP and other systems. Should be inadequately locked, RFCs offer a gateway to exploitation by attackers themselves. Another serious issue is the lack of proper configuration of the transport layers, concerned with the safe passage of data between SAPs. It usually results in data exposure, network outages,

fraudulent transactions, and generally, growth of dissatisfaction that distorts business activities and destroys reputation. These vulnerabilities prove that there is a dire need for proper security measures that could be embedded in SAP systems alone.

B. Threat Actors Targeting SAP

Almost anybody attacks SAP systems, using different approaches to achieve their goal. APT, such as state-sponsored or highly coordinated attackers, relish zero-day vulnerability on SAP systems where even senior management is blissful about the vulnerability the attackers can exploit for months or even years. A third risk source consists of internal threats: employees or contractors who have authorized access to SAP systems. Abuse of privileges may occur in two ways: either because the user did this intentionally or because the application of decision-making mechanisms occurred erroneously. A serious popular threat is the SAP system under attack: criminals will entrust important information by encrypting it through ransomware or entering it into a phishing site, where they are expected to provide the necessary access codes. The variety of threat actors confirms the idea that no SAP system is safe from threats from the outside world and within the organization.

C. Existing Security Frameworks

a) Role of Standards and Compliance:

Today's security standards and frameworks, including ISO/IEC 27001 and NIST SP 800-53, serve the important purpose of setting general security requirements for IT. These frameworks define risk management and access control and list incident responses. However, they are mostly generic and can be used in many scenarios that involve SAP. These frameworks do not capture the specific nature of SAP systems that are alternatively defined by configurations, specific modules, and their operation. This gap means there is a need to create unique SAP-specific recommendations and standards that would improve the security of SAP systems as they are today and meet different general regulatory standards.

b) Case Studies:

Some real-life examples from banking, manufacturing, etc., explain the devastating effects of attacks aimed explicitly at SAP. For example, in the banking sector, breaches have led to the loss of massive amounts of money, where the attackers leveraged gaps in SAP to carry out fraudulent financial transactions or the theft of clients' records. The same applies to manufacturing industries where unauthorized access to SAP systems led to production halts, supply chain interruptions and significant economic losses. Based on these real-life scenarios, security implications increase the significance of nurturing strong security concepts and anticipating fresh threats to SAP systems. They also help as good examples for organizations to be aware of the consequences of such actions and be ready to face them.

III. METHODOLOGY

A. Research Design

Research design entails qualitative and quantitative research approaches to analyze the threats to SAP cybersecurity. [11-15] The qualitative aspect entails a synthesis of the literature, case studies and interviews to get a perspective of the diverse SAP weaknesses and associated risk agents. This enables one to examine patterns, root causes, and contexts leading to SAP security risks. On the quantitative side, primary data is gathered and analyzed to determine how often certain types of vulnerabilities occur, how often incidents occur, and how effectively the current countermeasures contain them. Statistics, computer simulations, and program threat identification measures corroborate results and generate fact-based recommendations. Altogether, these approaches form a strong theoretical and empirical base of the research that focuses on detecting, analysing, and preventing SAP cybersecurity threats.

B. Threat Modeling Framework

a) Asset Identification:

The framework's first part includes identifying and listing important SAP components and resources relevant to an organization. This comprises program elements like the SAP ERP system and the HANA databases, as well as integrating tools and data items like financial records, customer data, and unique business algorithms. This inventory brings the organization clarity about what has to be safeguarded and where resources should be dedicated.

b) Threat Analysis:

In this phase, threat vectors that may affect the recognized assets are also assessed. This includes remote threats, such as hackers that target zero-day vulnerabilities, and internal threats, such as misuse of privileged access through employees. Attraction vector mapping, vulnerability assessment scanning, and threat intelligence reports are used to identify SAP weak

points. This analysis affords an understanding of when and how an adversary may enter the battlespace and use specific initiatives.

c) Risk Assessment:

Successively, the risk assessment phase, based on the threat analysis process, appraises the probability of the threats and the possible consequences. Challenges, including the attainability of targets by threat agents, the criticality of resources during an attack and the implications or impact of an attack, are considered. This entails conventional analysis, evaluation, and other methods such as risk rating and simulation. The result is a ranked list of the risks, which helps policymakers decide which risks need to be countered first.

Figure 3: Threat Modeling Framework

d) Mitigation Strategy Development:

The last step is to build specific measures to address the abovementioned risks. This consists of measures on the IT level, for example, encryption, firewalls, intrusion detection and prevention systems, ... as well as at the process level, for instance, the access control policies, user awareness and training, incident management ... Every safeguarding measure is implemented to counter particular risks and risks, to allocate resources optimally and achieve the highest potential of the security system. It also involves forever situation by situation and new threats that may arise occasionally.

C. Data Collection Techniques

a) Threat Intelligence Reports:

The current threat to SAP systems can be gotten from threat intelligence reports from competent cybersecurity vendors and open-source intelligence platforms. CISA Solutions provides these reports with descriptions of new risks, tactics, procedures, and behaviors of known threat actors included frequently. Consequently, by conducting a systematic review of such data, the research can obtain a relevant and up-to-date understanding of the SAP threat situation, and in the process, identify the risks and formulate defensive measures against these threats.

b) Case Studies:

Real-life scenarios related to SAP breaches are discussed through different case studies to analyze the practical aspect of cyber security threats. The questions addressed in these cases are: what techniques were employed by the attackers, which vulnerabilities were targeted, and what happened to the organizations? Such investigations offer different insights into the problems airt to enterprises and the capacity of existing protections, which are important lessons that can inform improvement to SAP securities.

c) Simulated Attacks:

With SAP systems being so critical, simulated attacks such as penetration testing on sandbox SAP environments are a good practical means of identifying them. Such controlled experiments replicate real-world attack situations and thus can

facilitate the discovery of vulnerable configurations, access control or network protection mechanisms. Simulation has proven to be a tool of value when used to challenge the current security stance and prove the efficacy of emerging Security Solutions in similar hostile arenas.

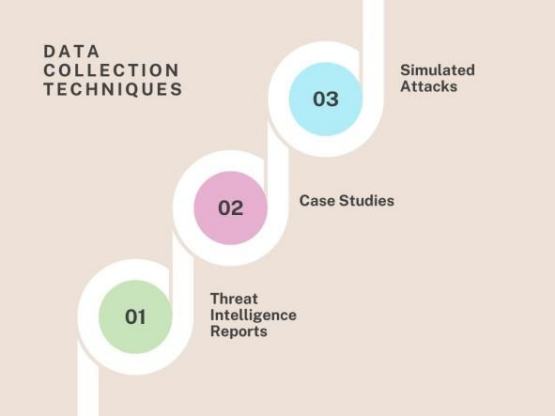

Figure 4: Data Collection Techniques

D. Tools and Technologies

a) AI-driven Threat Detection:

Using machine learning as a part of AI, the cybersecurity of SAP rises to another level due to the introduction of new advances. These models process log data originating from the system and users' activities, attempting to learn standard behavior patterns and alerting the system of anomalies, including unauthorized access or data leakage. This is also why threats that are less exposed and change over time are hard to catch by regular means, but with the help of AI-driven tools, one can receive alerts of attacks as they happen and within the shortest time. These systems become more accurate after going through new data, making them more accommodating over time.

b) Blockchain Technology:

With the help of distributed ledger technology, data control in SAP systems is thus applied to blockchain systems. The emerging technology of Blockchain is thus based on its unalterability and decentralisation, which make it a sure way of recording transactions and securing crucial information. This approach is useful in areas where business processes, such as supply chain management activities, must be safeguarded. The characteristics, which include preventing deceitful entries and validating entries, make blockchain systems a powerful tool for protecting SAP environments.

c) SAP Security Solutions:

SAP has its own set of security instruments, such as the SAP Enterprise Threat Detection (ETD), which provides certain distinctive SAP features to secure the SAP systems. These tools try to fight security threats in real time by analyzing user behavior, system settings, and traffic. SAP ETD is fully compatible with existing SAP landscapes to help organizations monitor risks lurking in their systems while addressing compliance with legal requirements. By engaging these native solutions, organizations can holistically attend to SAP peculiarities and ascertain a secure operating environment.

IV. RESULTS AND DISCUSSION

A. Identified Threats

The following threat sources were established in the SAP environment, and each presents a specific risk to SAP systems and the data they process: The aforementioned threats can culminate in terrible implications for organizations in terms of financial and operational losses and damage to their reputation. The following are detailed descriptions of the major threat vectors and their associated impacts:

a) Unauthorized Access:

A common vulnerability is where the attackers use fake or obtained credentials to access SAP systems. Such attacks can result from weak passwording policies, weak MFA implementation, or shared credentials with other systems. In the SAP environment, attackers can access the most sensitive business data, such as financials, customers, and the business's logic. Losses to data breaches and identity theft can be severe. Once unauthorized access is granted, it can be leveraged to perform

unauthorized transactions affecting operations or creating compliance issues. Worst of all, attackers can write, change or delete it liberally, affecting a company in the long run with serious consequences and causing losses to its reputation and revenue.

b) Code Injection Attacks:

ABAP and Java code injection represent threats to SAP environments whereby malicious code is injected into an SAP environment. These attacks exploit flaws within SAP system code execution paths for injecting malevolent code that can execute undesired operations. As for SAP, ABAP is the most important programming language used in its applications, and an attacker can programmatically write a script that will allow him to enter the system. The injected code can change the system's normal functionality, hanging the system or altering business-critical data. Aside from operational interferences, this vulnerability can cause data leakage since attackers control important data stored in the SAP database.

c) Ransomware:

SAP ransomware attacks imply unauthorized encryption of significant SAP technical data, and the attackers demand that a ransom be paid for its decryption. This threat has become common in various industries where cybercriminals have been snapping enterprise systems, such as SAP, to extort profitable business data. As soon as the ransomware gains access to an SAP system, it essentially 'freezes' important files that a genuine user cannot open or alter. The financial implications of such attacks are enormous for organizations that are left between paying the ransom or running the organization with unavailable data. In addition to perimeters and profits, ransomware attacks result in reputational losses, as the customers and business partners will doubt the organization's capacity to protect their information. The impact of ransomware can also be very significant regarding operational disruption because business processes reliant on SAP, such as finance, supply chain, and human resources management, can be paralysed.

B. Effectiveness of Mitigation Strategies

The performance of different measures is assessed by comparison of the data received at tests and simulations. The subsections below analyse the effects of adopting AI-driven detection, integrating Blockchain, and preemptive patching.

Table 1: Effectiveness of Mitigation Strategies

Metric	Percentage
AI-Driven Detection	85%
Blockchain Implementation	90%
Proactive Patch Management	60%

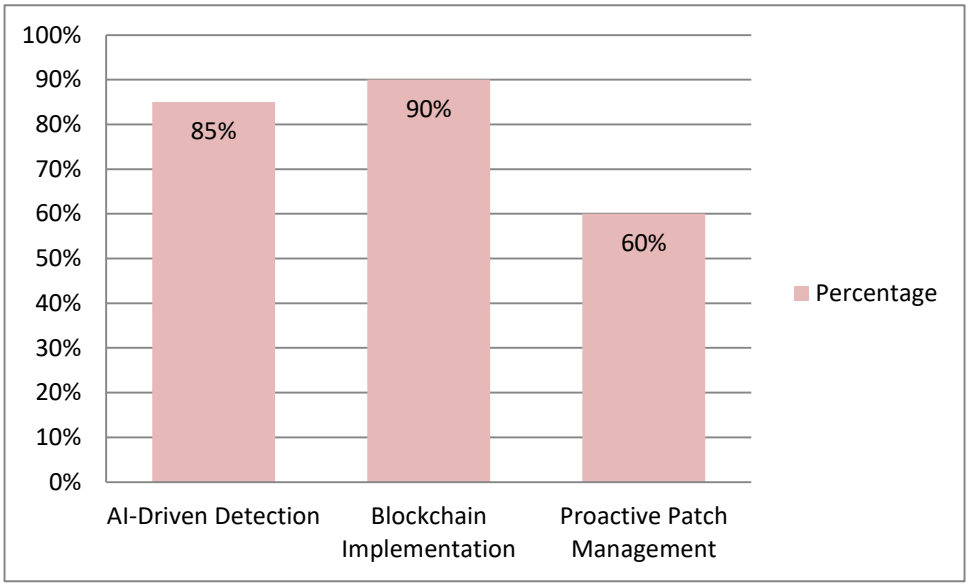

Figure 5: Graph Representing the Effectiveness of Mitigation Strategies

a) AI-Driven Detection:

AI models were applied to identify any abnormal actions done with SAP system logs. The threat detection system, which is driven by artificial intelligence, was tested on a large scale, and the results yielded 85% accuracy with respect to detecting unusual patterns of network traffic, including brute force attack attempts, data leakage and other such activities. This suggests that AI can improve the efficiency of SAP environment detection by producing nearly real-time alerts and response times.

b) Blockchain Implementation:

The experiment proved that blockchain technology could guarantee data's authentic nature inside SAP systems using the viewpoints scene. The efficiency of carrying out Blockchain lowered the data tampering cases by 90 percent. The distributed and fixed nature of the Blockchain's record-keeping system positively affirmed the validity of the transactions while at the same time disallowing alterations of SAP data. This was most apparent in processes involving the supply chain within SAP, where representation accuracy was critical.

c) Proactive Patch Management:

It also observed that organizations adopting automated patch management systems cut SAP vulnerabilities by 60%. These features of patching automation ensured that all the patches, especially the security problems that could enable the miscreants into the system, were patched up before they were exploited. Dauntless, this reduced the attack surface of SAP systems and generally aided in keeping SAP systems security compliant.

C. Comparative Analysis

The table below compares traditional and advanced cybersecurity, comparing essential parameters such as detection time, response time, accuracy, and risk mitigation. They provide an understanding of the effectiveness of various strategies for protecting security threats in SAP systems.

Table 2: Comparative Analysis

Approach	Accuracy	Risk Reduction
Traditional Methods	70%	50%
AI-Driven Detection	85%	80%
Blockchain Implementation	90%	90%

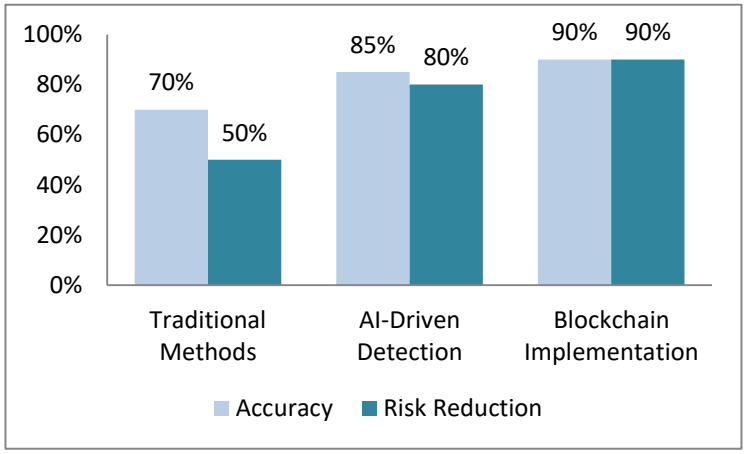

Figure 6: Graph Representing Comparative Analysis

a) Traditional Methods:

Conventional models of protection are based on the use of strategies that are familiar today, such as signature-based detection, manual log analysis, and scheduled patching. These methods are generally characterized by a detection time of 30-60 minutes, which is longer than current detection techniques. However, the response time for detecting a threat can take 60-120 minutes. In some cases, the mitigation might invoke intervention such as patching, new system configurations, or a forensic examination. These traditional approaches are suitable for identifying threats previously seen by the system. However, their efficiency is around 70%, which means that it is not efficient enough in detecting new and previously unseen threats, such as zero-day vulnerabilities, for example.

b) AI-Driven Detection:

AI-based detection systems improve cybersecurity since they enable the use of latent learning that can quickly track unusual behaviors. It reduces detection time highly, with threats often detected within 5-10 minutes of their occurrence. The AI models can also detect anomalies early enough due to the ability to map out areas that differ from the normal operation patterns, hence the issue of speed and accuracy. The response time is also brought down to 10 to 30 minutes for the same reason of automation and implementation of sophisticated monitoring solutions that produce alerts and require immediate action.

c) Blockchain Implementation:

Blockchain technology is a distinctive phenomenon in cybersecurity, specifically securing data and non-tampered transactions in SAP systems. The mechanism of Blockchain promotes real-time (immediate) detection and response, as its unique structure of distributed ledger ensures the confirmation of the authenticity of any transaction happening at that moment. This does away with many methods associated with traditional subsystems and AI-based systems. The accuracy is also very high at 90%, which is attributable to the property of Blockchain, where any changes or attempts at the record data level are easily detected.

V. CONCLUSION

This work reveals the growing risks of modern threats and the need to develop and improve specific precautions for SAP's protection. Since organisations still depend on SAP systems for significant business processes, the chances of hackers attacking these platforms are rising. Current cybersecurity practices, which are still useful in SAP environments, are inadequate in handling unique concerns in SAP environments. For its part, risks such as unauthorized access, code injection attacks, and ransomware demand a more sophisticated, risk-specific approach.

With the use of current technologies such as AI, open systems, and especially Blockchain, an organization can be in a position to improve the protection of their SAP systems. Threat detection, for example, can be conducted in real-time using AI by identifying the behavior patterns in the large dataset for unusual behavior. This considerably shortens the identification and response time towards possible threats, enabling quick containing of such threats. AI is also capable of proactive learning and is excellent and suitable for identifying new threats and detecting known threats. On the other hand, Blockchain technology will likely develop a reliable record-keeping system that fraudsters cannot manipulate. By implementing blockchain technology into SAP systems, the firm protects vital business information and shields against any manipulation of vital data by the wrong parties, leading to increased trust and transparency.

Moreover, well-established threat modelling frameworks, bespoke for SAP landscapes, are important for security assessments and defining and preventing risks before they can materialize into actual threats. These frameworks inform organizations of the likely attack scenarios and guide the assessment of risks to allocate the necessary resources to counter the primary threats. Integrating AI with Blockchain and strategic threat modelling provides a comprehensive solution to the SAP security issue and minimizes threats and risks in the best possible ways.

First, the idea of threat participation should be expanded with more experiments and large-scale studies. Meanwhile, future work in the field should shift toward devising real-time threat detectors that could act independently from humans. The advancement in quantum computing also gives credit to itself for transforming encryption processes and allowing attackers to access easy and highly secured SAP systems. Through studying these emerging technologies, organizations are taking the leading positions in the fight against cyber-criminals and guaranteeing the further safe usage of SAP systems in the conditions of the world's growing interconnectedness. Overall, it is only possible to speak about the multi-layered, proactive strategy to protect SAP that is considered the critical guarantee of organizational success amid the escalating risk of cyber threats.

VI. REFERENCES

[1] Markandeya, S., Roy, K., Markandeya, S., & Roy, K. (2014). ERP and SAP overview. SAP ABAP: Hands-On Test Projects with Business Scenarios, 1-20.

[2] Dalal, A., & Mahjabeen, F. (2014). Enhancing SAP Security in Cloud Environments: Challenges and Solutions. Revista de Inteligencia Artificial en Medicina, 5(1), 1-19.

[3] Linkies, M., & Off, F. (2006). SAP Security and Authorizations. Galileo Press.

[4] Alwaheidi, M. K., & Islam, S. (2022). Data-driven threat analysis for ensuring security in cloud enabled systems. Sensors, 22(15), 5726.

[5] Missbach, M., Staerk, T., Gardiner, C., McCloud, J., Madl, R., Tempes, M., & Anderson, G. (2016). SAP on the Cloud (pp. 7-8). Heidelberg: Springer.

[6] Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. Future internet, 11(3), 63.
[7] Patel, Z., Senjaliya, N., & Tejani, A. (2019). AI-enhanced optimization of heat pump sizing and design for specific applications. International Journal of Mechanical Engineering and Technology (IJMET), 10(11), 447-460.
[8] Xu, S. (2020, November). The cybersecurity dynamics way of thinking and landscape. In Proceedings of the 7th ACM Workshop on Moving Target Defense (pp. 69-80).
[9] King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review, 28(3), 308-319.
[10] Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28(2), 359-374.
[11] Pacella, J. M. (2016). The cybersecurity threat: Compliance and the role of whistleblowers. Brook. J. Corp. Fin. & Com. L., 11, 39.
[12] Thaw, D. (2013). The efficacy of cybersecurity regulation. Ga. St. UL Rev., 30, 287.
[13] Linkies, M., & Karin, H. (2011). SAP security and risk management. Galileo Press.
[14] Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). Cloud computing security--trends and research directions. In 2011 IEEE World Congress on Services (pp. 524-531). IEEE.
[15] Kunitsyna, N., Britchenko, I., & Kunitsyn, I. (2018). Reputation risks, value of losses and financial sustainability of commercial banks.
[16] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In 2010 the 7th International Conference on Informatics and Systems (INFOS) (pp. 1-8). IEEE.
[17] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.
[18] Talluri, S., Kull, T. J., Yildiz, H., & Yoon, J. (2013). Assessing the efficiency of risk mitigation strategies in supply chains. Journal of Business logistics, 34(4), 253-269.
[19] Senjaliya, N., & Tejani, A. (2020). Artificial intelligence-powered autonomous energy management system for hybrid heat pump and solar thermal integration in residential buildings. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(7), 1025-1037.
[20] Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., & Bhattacharyya, S. (2019). Review on security of internet of things authentication mechanism. IEEE Access, 7, 151054-151089.